

Общая Алгебра.

Вопрос №1.

Декартово произведение мн-в и бинарное отношение. Отношение эквивалентности. Фактор мн-во.

Опр. Декартовым произведением множеств X и Y наз-ся мн-во всевозможных упорядоченных пар (x, y) , в которых $x \in X, y \in Y$

$$X \times Y = \{ (x, y) \mid x \in X; y \in Y \}$$

Замеч. $X \times X$ - дек-вый квадрат X
 (x, x) - диагональ дек. квадр.

Примеры: $\mathbb{Q}$ можно рассм. как $\mathbb{Z} \times \mathbb{N}$

Опр. Говорят, что на мн-ве X задано бинарное отношение R , если указано непустое подмножество R дек-ва квадрата этого мн-ва. Если при этом $(x, y) \in R$, то говорят, что x и y связаны отношением R ($x R y$).

Бинарное отношение наз-ся:

- рефлексивным, если $x R x \quad \forall x \in X$;
- симметричным, если $x R y \Rightarrow y R x$;
- транзитивным, если $x R y, y R z \Rightarrow x R z$;

Опр. Бинарное отношение E на мн-ве X наз-ся отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Если x и y эквивалентны, то это обозн. $x \sim y$ ($x \mathrel{R} y$)

Опр. Пусть на мн-ве X задано отношение эквивалентности E и $a \in X$. Мн-во всех эл-ов $x \in X$, эквивалентных a наз-ся классом эквив., порожденным эл-ом a .

$$cl(a) = \{x \in X \mid x \mathrel{R} a\}$$
$$[R(a)]$$

$\forall$ эл-м - наз-ся представителем класса.

Теорема 1. Класс эквивалентности порождается любым своим представителем, т.е. если $b \in cl(a)$, то $cl(b) = cl(a)$.



Док-во:



$c \in cl(b) \Rightarrow c \sim b$, но $b \sim a \Rightarrow c \sim a \Rightarrow c \in cl(a)$
 $c \in cl(a) \Rightarrow c \sim a$, но $a \sim b \Rightarrow c \sim b \Rightarrow c \in cl(b)$

Теорема 2. Два класса эквивалентности либо не пересекаются либо совпадают.



Док-во: $\forall$ два класса $cl(a)$ и $cl(b)$ либо не пересекаются, либо имеют хотя бы один общий эл-м, но в этом

случае они совпадают, т.е. если $c \in c(b)$ и $e \in c(a)$, то $c(a) = c(b)$

Опр Мн-во всех классов эквивалентности (теор 1)

наз-ся Фактор мн-ва мн-ва X по отношению эквивалентности E .

Обозн.: X/E .

Пример:

Пусть $p \in \mathbb{N}; p > 1$;
 Пусть $m \sim n$, если $m \equiv n \pmod{p}$ мн-во чисел n кон. при делении на p дает ост. n
 $m/p = pk + r: c(b)(m) = \{ n = pk + r \mid k \in \mathbb{Z} \}$
 Все классы: $C_r = \{ n = pk + r \mid k \in \mathbb{Z} \} \quad 0 \leq r \leq p-1$

Фактор мн-ва: $\mathbb{Z}_p = \{ c_0, c_1, \dots, c_{p-1} \}$

$\uparrow$
 мн-во классов вычетов по модулю p

Зам.: Мн-во - совокупность об-ов, наз-х эл-ми мн-ва.

Опр S - собственное подмн-во мн-ва X , если: $\begin{cases} S \subset X; \\ S \neq \emptyset; \\ S \neq X; \end{cases}$

Опр Разность мн-в X и Y - мн-во тех x , которые нет в Y :

$$X \setminus Y = \{ x \mid x \in X, x \notin Y \}$$

Если $Y \subset X$, то $X \setminus Y$ - дополнение мн-ва Y до X ($Y, C_X Y, C_Y$)

Вопрос №2.

Отображения. Обратное отображение.

Опр. X, Y - два мн-ва;

Отображением f мн-ва X на мн-во Y наз-ся закон, посредством которого каждому $x \in X$ ставится в соответствие однозначно опр-ый эл-т $y \in Y$

y - образ эл-та x ;
 x - прообраз эл-та y ;

Запись: $f: X \rightarrow Y$

Отображение мн-ва X в мн-во Y наз-ют так-же:

- преобразованием мн-ва X в Y
- оператором действ. из X в Y
- функцией опр-ой на X со значениями из Y

Опр. Полным прообразом эл-та $y \in Y$ наз-ся мн-во:

$$f^{-1}(y) = \{x \in X \mid f(x) = y\};$$

Образом отображения f наз-ся мн-во:

$$\text{im } f = \{y = f(x) \mid x \in X\} \\ [f(X)]$$

Опр. Отображение $f: X \rightarrow Y$ называется:

1) Инъективным

Если $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

(другими словами, $y = f(x)$ имеет не более одного решения)
 $\forall y \in Y$

2) Сюръективный (отображение на)

Если $\text{Im} f = Y$

(другими словами, если $f(x) = y$
 $\forall y \in Y$ имеет хотя бы одно реш.)

3) Биективный

Если f — сюръективный и инъективный
(друг. словами $y = f(x)$ $\forall y \in Y$ имеет ед. реш.)

Опр. Два отображения $f: X \rightarrow Y$ и
 $g: X \rightarrow Y$ наз-ся равными, если
 $f(x) = g(x) \quad \forall x \in X$

Тождественное (единичное)

отображением на мн-ве X наз-ся
отобр. $e_X: X \rightarrow X$, для которого
 $e_X(x) = x$ для $\forall x \in X$;

Произведение отображений:

Опр. Произведения (суперпоз.) отображ.
 $g: X \rightarrow Y$ и $f: Y \rightarrow Z$ наз-ся
отображение $fg: X \rightarrow Z$, опр-е:

$$\underline{fg}(x) = f(g(x)) \quad \forall x \in X$$

Свойства:

1. $f e_X = f$; $e_Y f = f$, где
 $\forall f: X \rightarrow Y$

2. Пр-е отображение ассоциативно,
т.е. если $h: X \rightarrow Y$; $g: Y \rightarrow Z$; $f: Z \rightarrow U$,

то
$$F(gh) = (fg)h;$$

Док-во:

В соотв-е с опр. равенства отображений
сравним значения.

$$F(gh): X \rightarrow U \quad \text{и} \quad (fg)h: X \rightarrow U \quad \forall x \in X, \text{ где-то имеем:}$$
$$(f(gh))(x) = f((gh)(x)) = f(g(h(x))) =$$
$$= (fg)(h(x)) = ((fg)h)(x)$$

3. Произведение инъективных (сюръект.,
бъективных) отображений инъективно
(соотв-но сюръективно, бъективно).

Док-во:

1) $g: X \rightarrow Y$; $f: Y \rightarrow Z$ - инъективные
отобр.;
Пусть $x_1 \neq x_2$, тогда:
 $g(x_1) \neq g(x_2)$ и $f(g(x_1)) \neq f(g(x_2))$,
т.е. $fg(x_1) \neq fg(x_2)$;

2) Пусть f и g - сюръективны $\Rightarrow$
 $\forall z \in Z \quad \exists y \in Y: z = f(y)$, то для
этого $y \quad \exists x \in X: y = g(x) \Rightarrow$
 $\forall z \in Z \quad \exists x: z = f(g(x))$, т.е. $z = fg(x)$;

3) Бъективность вытекает из 1) и 2).

Обратное отображение:

$$f: X \rightarrow Y;$$

Опр. Отображение $f^{-1}: Y \rightarrow X$ наз-ся обратным к отобр. f , если

$$f^{-1}f = e_X; \quad ff^{-1} = e_Y$$

Отображение для которого существует об-ое - обратное.

Теорема 1. Отображение обратимо тогда и т. тогда, когда оно биективно.

Д-во

Лемма Если $g: X \rightarrow Y, f: Y \rightarrow X$ и $fg = e_X$, то g инъективно, а f - сюръективно.

Доп-во леммы:

• Пусть g не инъективно, тогда:

$\exists x_1, x_2 \stackrel{x_1 \neq x_2}{=} g(x_1) = g(x_2)$, но тогда:

$$x_1 = e_X(x_1) = f(g(x_1)) = f(g(x_2)) = e_X(x_2) = x_2 \Rightarrow g - \text{инъективно.}$$

• $\forall x \in X: x = e_X(x) = fg(x) = f(g(x)) = f(y)$,

где $y = g(x) \in Y \Rightarrow f$ - сюръективно,

Необходимость $\Rightarrow$

Пусть f - обратимо

Тогда f инъективно и сюръективно на основании леммы $\Leftrightarrow f$ - биективно,

Достаточность $\Leftarrow$

Пусть f - биективно,

Тогда $\forall y \in Y \exists! x \in X$.

Рассмотрим отображение $g: Y \rightarrow X$, такое что $g(y) = x$.

Тогда для $\forall y \in Y: (fg)(y) = f(g(y)) = f(x) = y$, т.е. $fg = e_y$, а для:

$\forall x \in X: (gf)(x) = g(f(x)) = g(y) = x$, т.е. $gf = e_x \Rightarrow$

$g = f^{-1}$ и f — обратное,

Об-ва обратных отображ.:

1. Обратное отображ. единственно:

Пусть f_1^{-1}, f_2^{-1} — оба обр.-ых отображ. к отображ. $f: X \rightarrow Y$

Тогда $f_1^{-1} = f_1^{-1} \cdot e_x = f_1^{-1}(ff_2^{-1}) = (f_1^{-1}f)f_2^{-1} = e_x f_2^{-1} = f_2^{-1}$;

2. Произведение обратных отображ. — обратное
[при этом: $(fg)^{-1} = g^{-1}f^{-1}$]

fg — обратное, как произведение биективных отображ., при этом:

$$(fg)(g^{-1}f^{-1}) = f(gg^{-1})f^{-1} = ff^{-1} = e_y;$$

$$(g^{-1}f^{-1})(fg) = g^{-1}(ff)g = g^{-1}g = e_x;$$

Вопрос №3

Алгебраические операции.

Обобщенный закон ассоциативности.

Внутренний закон композиции:

Опр. Внутр. з. композиции (алгебр. операции) на мн-ве X наз-ся отображение

$$* : X \times X \rightarrow X$$

символ. запись: $a * b = c$;

Алгебр. операция, наз-ся коммутативной,
если: $a * b = b * a$, $\forall a, b \in X$;

если $(a * b) * c = a * (b * c)$, $\forall a, b, c \in X$; ассоциативной,

Обобщенная ассоциативность:

Теорема 1 Если алгебраическая операция $*$ на мн-ве X - ассоциативна, то результат ее применения не зависит от расстановки скобок, лишь бы скобки объединяли пары эл-ов, указывая на порядок последовательного применения опер к 2 эл-ам.

Д-во:



Докажем индукцией по n .

Для $n=3$ - очевидно;

Пусть верно для $\forall k < n$;

Доказ-м для $k=n$:

Пусть в $a_1 * \dots * a_n$ произвольно расставлены скобки;

последним шагом будет всегда выполнение операции над двумя $\mathbb{N}$ -ми:

$$a_1 * \dots * a_k \text{ и } a_{k+1} * \dots * a_n$$

($1 \leq k \leq n-1$), так как $k < n$, то оба выражения не зав-т от распр. скобок. Останется показать, что:

$$(a_1 * \dots * a_k) * (a_{k+1} * \dots * a_n) =$$

$$= (a_1 * \dots * a_m) * (a_{m+1} * \dots * a_n);$$

$$\text{где } 1 \leq m \leq n-1$$

Пусть $k < m$ обозначим

$$a_1 * \dots * a_k = a;$$

$$a_{k+1} * \dots * a_m = b, \quad a_{m+1} * \dots * a_n = c;$$

Надо показать, что

$$a * (b * c) = (a * b) * c;$$

А это верно! Опр. $e \in X$ - нейтр. $\mathbb{N}$ -м мно-ва X относ опер. $*$, если $\forall a \in X$:
 $a * e = e * a = a$;

Теорема 2 Нейтральной $\mathbb{N}$ -м - единствен.

Доказ-во: e_1 и e_2 - два нейтр. $\mathbb{N}$ -ма;

$$e_1 * e_2 = e_1 \text{ и } e_1 * e_2 = e_2 \Rightarrow$$

$$\underline{e_1 * e_2};$$

Теорема 3 Симметричный эл-т относительно ассоциативной алгебр. операции единствен.

Опр. x' симметр. эл-т для x , если: $xx' = x'xe$

Док-во: Если x' и x'' - два симметр. эл-та к эл-ту $x \in X$, то

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x'';$$

Опр. Алгебр. опер. $*$ на мн-ве X обладает обратной операцией если для $\forall a, b \in X$ уравнения $a * x = b$ и $y * a = b$ имеют ед. решение.

• Наличие обратной операции $\Leftrightarrow$ наличие правой обратной и левой обратной
 $\forall a, b \in X \exists x: ax = b \quad \exists y: ya = b$

Опр. $*_1$ и $*_2$ - две асо. операции на мн-ве X . Алгебр. опер. $*_1$ наз-ся дистрибутивной справа относительно алгебр. операции $*_2$, если

$$\forall a, b, c \in X: (a *_2 b) *_1 c = (a *_1 c) *_2 (b *_1 c);$$

дистрибутивной слева:

$$\forall a, b, c \in X: a *_1 (b *_2 c) = (a *_1 b) *_2 (a *_1 c);$$

Внешний закон композиции:

Пусть X и P - два мн-ва:

Опр.

Внешний законом композиции на мн-ве X наз-ся отображение:

$$P \times X \rightarrow X$$

т.е. закон, по которому:

$$\forall \alpha \in P \text{ и } \forall x \in X : \exists! c \in X : \\ (\alpha, x) \mapsto c$$

Обозн: $c = \alpha x$

Опр

2) Внешн. з. композиции на мн-ве X наз-ся дистрибутивный относ. внутр. закон композиции $\ast'$ в P , если

$$\forall a \in X; \forall \alpha, \beta \in P (\alpha \ast' \beta) a = \alpha a \ast' \beta a$$

1) Внешний з. композиции на мн-ве X наз-ся дистрибутивный относ. внутр. закон композиции $\ast$ в X , если:

$$\forall \alpha \in P, \forall a, b \in X : \alpha(a \ast b) = \alpha a \ast \alpha b$$

Вопрос №4

Группы. Основное св-во.

Опр.:

Непустое мн-во G с заданной на нем алгебраической операцией $*$ наз-ся группой, если:

1) $(a * b) * c = a * (b * c); \forall a, b, c \in G$
(ассоциативность)

2) $\exists e \in G : a * e = e * a = a \quad \forall a \in G$
(опер. обладает нейтрал. эл-том)

3) $\forall a \in G \exists a' \in G :$

$$a * a' = a' * a = e,$$

Сбозн.: G или $\langle G, * \rangle$

Опр.:

Группа с коммутативной операцией наз-ся абелевой.

Св-ва:

1) $\forall$ группе $\exists! e : a * e = e * a = a;$

2) $\forall$ группе $\exists! a' : a * a' = a' * a = e;$

$e_n \in G : a * e_n = a$ - правая единица

$a_n^{-1} \in G : a * a_n^{-1} = e_n$ - правый обр. к эл-ту a

Теорема 1. Мн-во G с ассоциативной операцией явл-ся группой, если оно обладает правой единицей e_n и по отношению к ней, каждый эл-т

$a \in G$ обладает правом обратным.



Доказательство:

Пусть a - произв. эл-т мн-ва G
 a^{-1} - обратным к нему

Тогда: $a a^{-1} = e_n = e_n e_n = e_n (a a^{-1}) = (e_n a) a^{-1}$

$$a a^{-1} = (e_n a) a^{-1}; \quad | \cdot (a^{-1})^{-1}$$

$$a \cdot \underbrace{(a^{-1} (a^{-1})^{-1})}_{e_n} = (e_n a) \cdot \underbrace{(a^{-1} (a^{-1})^{-1})}_{e_n},$$

т.е. правая единица мн-ва G
оказывается и левой ед., т.е.
просто единицей e мн-ва G .

2) Показ-м: $a^{-1} a = e$

$$e a^{-1} = a^{-1} e = a^{-1} (a a^{-1}) = (a^{-1} a) a^{-1};$$

$$e a^{-1} = (a^{-1} a) a^{-1} | \cdot (a^{-1})^{-1};$$

$$e = a^{-1} a, \text{ верно!}$$

Следствие:

В группе G правая e явл-ся левой и единств.
единицей, которой обл. эта гр. То же самое
справедливо и для правого обр. эл-та.

Теорема 2.

Мн-во G с ассоциативной
операцией явл-ся группой $\Leftrightarrow$
эта операция обладает обратной

До во:



$\Rightarrow$ G - группа, покажем, что $ax=b$ (1) имеет
ед. решение для $\forall a, b \in G$.

Действительно: $\exists$ л-м $x = a^{-1}b$ явл-ся
решением (1), т.к. $ax = a(a^{-1}b) = eb = b$, это
решение единственно, т.к., если x' - другое
реш., то

$$\begin{aligned} ax' &= ax; \\ \underbrace{a^{-1}a}_{e} x' &= \underbrace{a^{-1}a}_{e} x; \\ x' &= x \end{aligned}$$

Аналогично.

$$y = ba^{-1} - \text{ед. решение (2)}$$

$\Leftarrow$ Пусть (1) и (2) при $\forall a, b \in G$ имеют
ед. решение, покажем, что G - группа.

Для этого проверим выполн. условий теор. 1.

Возьмем произв. $a \in G$, тогда по усл.:

уравн. $ax=a$ имеет ед. решение;

Очевидно - это решение - прав. ед. для эл-та a :

$$e_a^a$$

Для $\forall$ другого эл-та $b \in G \exists y \in G: b = ya$
(т.е. y - решение (2))

$$\text{Тогда: } b = ya = y(a e_a^a) = (ya) e_a^a = b e_a^a \Rightarrow$$

$$\Rightarrow b = b e_a^a \quad \forall b \in G \Rightarrow e_a^a = e_n - \text{прав. ед. для } G;$$

Далее: $ax = e_n$ имеет ед. реш., которое
явл-ся прав. обр-ой к эл-ту a по отношению к e_n

А значит - в силу теор. 1, G - группа.



Замечание: Там не год-но, что в вырах
(невер) должна быть одна и та же
переб (невер) ед. гр. групп.

$$x = b + (-a)$$

- перебо бон.

$$y = (-a) + b$$

- перебо бон.

(разные пере
и перебо)

Вопрос №5

Подгруппы. Симметрическая и знакопеременные группы

Опр-ие.

Непустое подмножество H группы G называется подгруппой группы G , если оно само является группой относительно алгебраической операции в G .

Примеры

- 1) Тривиальная подгр: вся группа и ~~единичная~~ единичная $\{e\}$
- 2) Множество целых чисел $\langle \mathbb{Z}, + \rangle$ - подгр.
- 3) $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$ - подгр. $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$

Теорема 1.

Подмножество H группы G является подгр. этой группы $\Leftrightarrow$ имеет место:

- 1) $a, b \in H \Rightarrow ab \in H$;
- 2) $a \in H \Rightarrow a^{-1} \in H$;

Доказ.

$\Rightarrow$ Очевидно, т.к. H - группа;

$\Leftarrow$ Из 1) $\Rightarrow$ алгебр. операция в G является алгебр. операцией в H .

Пусть $a \in H$, тогда: (по 1) и 2))

$$a^{-1} \in H \text{ и } aa^{-1} \in H \Rightarrow e \in H.$$

Вопрос №5

Подгруппы. Симметрическая и знаменательные группы.

Опр.-ие.

Непустое подмножество H группы G называется подгруппой группы G , если оно само является группой относительно алгебраической операции в G .

Примеры

- 1) Тривиальная подгр.: вся группа и
- 2) $\langle \mathbb{Z}, + \rangle$ — подгр. ~~единичной~~ $\mathbb{Z}$ — подгр.
- 3) $\langle \mathbb{Q} \setminus \{0\}, \cdot \rangle$ — подгр. $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$

Теорема 1.

Подмножество H группы G является подгр. этой группы $\Leftrightarrow$ имеет место:

- 1) $a, b \in H \Rightarrow ab \in H$;
- 2) $a \in H \Rightarrow a^{-1} \in H$;

З-во:



Очевидно, т.к. H — группа;



Из 1) $\Rightarrow$ алгебр. операция в G является алгебр. операцией в H .

Пусть $a \in H$, тогда: (по 1) и 2)

$$a^{-1} \in H \text{ и } aa^{-1} \in H \Rightarrow e \in H.$$

Симметрическая гр. n -го порядка:

Мн-во S_n всех перестановок n -го порядка образует мультипликативную группу как мн-во всех биективных отображений мн-ва на себя.

(Породок гр. - $n!$)

Примеч.: мн-во $S(X)$ всех биективных отображ. $f: X \rightarrow X$ - мультиплик. неаб. группа.

Закопер-ая группа n -го порядка:

Мн-во A_n всех четных перестановок n -го пор-ка обр-ет мультиплик. группу.

Доказ-во:

Пока-м: A_n - подгруппа S_n

1. Пусть:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} \in A_n, g = \begin{pmatrix} 1 & 2 & \dots & n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix} \in A_n$$

т.е. $(\alpha_1, \dots, \alpha_n)$ и $(\beta_1, \dots, \beta_n)$ - четные перест. из первых n натур. чисел.

Пока-м: $fg \in A_n$

Заметим f в big : $f = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$

Тогда:

$$fg = \begin{pmatrix} 1 & 2 & \dots & n \\ \gamma_1 & \gamma_2 & \dots & \gamma_n \end{pmatrix} \in A_n, \text{ т.к.}$$

$(\gamma_1, \gamma_2, \dots, \gamma_n)$ - ненулевая перестановка из перестановок n канонич. чисел, т.е. существует единств. ненулевая α перестан. $(\beta_1, \dots, \beta_n)$

2. Определитель:

$$f = \begin{pmatrix} 1 & \dots & n \\ \alpha_1 & \dots & \alpha_n \end{pmatrix} \in A_n, \text{ но } f^{-1} = \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ 1 & \dots & n \end{pmatrix} \in A_n$$

$$\text{порядок гр. } A_n = \frac{n!}{2} \quad (n \geq 2)$$

Вопрос №6

Группа невырожд. матриц. Группа невырожд. Δ -ых матриц.
Группа ортогонал. матриц.

$$1) \langle \{A \in \mathbb{R}^{n \times n} \mid \det A \neq 0\}, \cdot \rangle$$

Проверим аксиомы группы:

1. Группов. матрицы - ассоциативны;

2. Нейтральный n -ик: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

3. Обратный n -ик: $\forall A: \exists! A^{-1} \quad AA^{-1} = A^{-1}A = I;$
т.е. $|A| \neq 0$;

2) Группа невырожд. верхних (нижних) Δ -ых матриц.

Покажем, что это подгруппа 1):

а) A, B - верхние Δ -ые матрицы:

k -ый столбец матрицы AB есть линейная комбинация первых k столбцов матрицы $A \Rightarrow$
все n -ица ниже k и строки равны 0 $\Rightarrow$
 AB - верхнетреугольная матрица.

б) (невырожд. AB - обратима)

Если A - невырожд. верхняя Δ -ая матрица, то
 k -ый столбец матрицы A^{-1} есть решение
системы уравнений $Ax = e_k$ (все квадрат. n -ица
 A равны 0).

Решая эту систему "снизу вверх"

Получим:

$$x_n = x_{n-1} = \dots = x_{k+1} = 0;$$

т.е. A^{-1} - верхняя A -св. матрица.
невероятно. A^{-1} - симметрична.

Получим, что это действ. подгруппа I).

3) Группа ортогональных матриц
Мн-во M всех ортогональных матриц
 $Q \in \mathbb{R}^{n \times n}$ обр-ет мультипликативную
группу т.е.:

а) Произв. ортогональных матриц - ортогональная матрица.

$$(Q_1 Q_2)^T Q_1 Q_2 = Q_2^T Q_1^T Q_1 Q_2 = I;$$

$$Q_1 Q_2 (Q_1 Q_2)^T = Q_1 Q_2 Q_2^T Q_1^T = I;$$

б) Обратная к ортогональной - ортогональная матрица:

$$Q^{-1} = Q^T \quad Q^T (Q^T)^T = Q^T Q = I.$$

$$(Q^T)^T Q^T = Q Q^T = I.$$

И согласно Теор. 1. (См. 5) M -
подгруппа мультипликативной группы невырожд.
матриц

Вопрос № 1

Конечные группы. Теорема Лагранжа.

Опр Конечная группа - состоит из конечного числа эл-ов.

Число эл-ов - порядок группы. ($\text{card } G$)

Примеры:

1. Группа из одного эл-та состоит только из единицы: $G = \{e\}$

*	e
e	e

$e * e = e$

2. Группа из двух эл-ов $G = \{e, a\}$

*	e	a
e	e	a
a	a	e

3. Группа из трех эл-ов $G = \{e, a, b\}$

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$$ab \neq a; \quad ob \neq b$$

$$ba \neq a; \quad ba \neq b$$

a или b - единица

1, 2, 3 - абелевы группы.

Теорема 1 (ЛAGRANЖA)

Во всякой конечной группе порядок ее подгруппы является делителем порядка самой группы.



Д-во:

Пусть $\text{card } G = n$, $\text{card } H = k$;

Рассмотрим левостороннее разложение группы G по подгруппе H . Оно состоит из всех левых смежных классов aH , где $a \in G$.

Каждый класс aH состоит из всех эл-ов ah , где $h \in H$. Все эл-ты ah различны (т.е. если $ah_1 = ah_2$, то $a^{-1}ah_1 = a^{-1}ah_2$ и $h_1 = h_2$), поэтому каждый aH состоит ровно из $\text{card } H = k$ эл-ов, общее число таких смежных классов $m \leq n$.

Таким образом, кол-во всех эл-ов G :

$$mk = n \Rightarrow n : k$$



Вопрос № 8

Степени эн-на Циклическая группа. Подгруппы цик. гр

В $\forall$ группе G могут быть опр-ны степени эн-на $g \in G$ (с целым показ):

$$g^k = \begin{cases} \underbrace{gg \dots g}_{k \text{ раз}}, & k > 0; \\ e, & k = 0; \\ \underbrace{g^{-1}g^{-1} \dots g^{-1}}_{k \text{ раз}}, & k < 0 \end{cases}$$

(в аддитивной группе вместо степеней говорят о кратности эн-а a и обозначают, как na)

$$\forall m, n \in \mathbb{Z} : a^n a^m = a^{n+m};$$

$$(a^n)^m = a^{nm};$$

(свойств: $na+ma=(n+m)a$ и $n(ma)=(nm)a$)

Теорема 1. Мно-во $\{a\}$ всех целых степеней эн-на a группы G образует абелеву группу.

До-во:

$\{a\}$ - подгруппа G , т.к.

$$a^n \in \{a\} \text{ и } a^m \in \{a\}, \text{ то } a^{n+m} \in \{a\}$$

$$a^{-m} = (a^{-1})^m = (a^m)^{-1};$$

Группа $\{a\}$ - циклическая группа, порожд. эн-ом a .

a - образующий эн-т.

Группа $\{a\}$ является подгруппой $\forall$ другой подгруппы группы G , содержащей эн-т a .

Теорема 2

Любая подгруппа циклической группы $\{a\}$ абн-я циклической.

Д-во:

Пусть H - подгр цикл. группы $\{a\}$, т.е. H состоит из нек-ых целых степеней эл-а a . $H = \{a^{k_1}, a^{k_2}, a^{k_3}, \dots\}$

Пусть m - наименьшее по абс. знач. число среди k_1, k_2, k_3 . Очевидно: H содержит все эл-ы вида a^{km} ($k \in \mathbb{Z}$)

Док-м, что в H не может быть других целых степеней эл-а a .

Пусть: $a^n \in H$. Разделим n на m , т:

$$n = mk + r \quad (m, r, k \in \mathbb{Z})$$

$$0 \leq r < m$$

$$\text{Тогда: } a^r = a^n \cdot a^{-mk}$$

Т.к. $a^n \in H$, $a^{-mk} \in H$, то $a^r \in H$, а это противоречит тому, что m - мин. степень (по абс. знач.) в H .

Пор-ок эл-та:

Если все степени эл-а различны, то a - эл-т бесконечного пор-ка, в противном случае - эл-т конечного пор-ка.

Теорема 3. Если a — n -м. ненулевого
пор-ка, то $\exists n \in \mathbb{N} : a^n = 1$ (в. оддитив.
группе: $na = 0$)

До-во: Пусть a — n -м. ненулевого
пор-ка, т.е. $\exists k, l \in \mathbb{Z} : a^k = a^l, k > l$ □

Тогда: $a^{k-l} = 1$, т.е. $\{n = k-l\} \in \mathbb{N}$.
 $a^n = 1$; ■

Наименьшее n , для кот-ого $a^n = 1$ —
порядок n -на a .

Теорема 4 Порядок n -на a группы
совпадает с пор-ом циклической подгр
 $\{a\}$.

До-во: Если пор-ок a равен n , □
то степени $a^0, a^1, \dots, a^{n-1}$ различны,
а всякая другая степень совпадает
с одной из этих n -ов. ■

Следствие 1 В конечной группе порядок любого
 n -а делителя делит пор-ка группы.

Следствие 2. Все конечные группы простого
пор-ка аб-я циклическими.

Следствие 3 В конечной группе G
пор-ка n :

$$a^n = 1 \quad (\forall a \in G);$$

Теорема 5. Эп-м a^k явл-ся образующим
 эп-ом численной группы $\{a\}$
 n -го порядка $\Leftrightarrow k$ и n взаимно
 просты.

□ До-во:

Пусть $d = \text{HCOB}(k, n)$ и

$$\begin{cases} n = dn' & (n' \leq n) \\ k = dk' & (k' \leq k) \end{cases}$$

Тогда эп-м a^k будет обр-м эп-ом числ-ой
 группы $\{a\} \Leftrightarrow$ пор-ок эп-ма a^k совпа-
 дает с n .

Так как: $(a^k)^{n'} = a^{kn'} = a^{dk'n'} = (a^n)^{k'} = 1$

$\rightarrow n = \frac{k}{k'} n'$
 $k n' = nk'$

То пор-ок a^k будет совпадать с $n \Leftrightarrow$
 $n' = n$, т.е. $d = 1$.

Вопрос №9

Подгруппы, смежные классы, норм. делители.

1. Подгруппы — см. Вопрос №5.

2. Смежные классы

Произведение подгрупп:

G — группа, M, N — две подгруппы

Произведением MN этих подгрупп наз-ся:

$$MN = \{ mn \mid m \in M, n \in N \}$$

(Если $M = \{ m \}$, то MN обозн. mN)

Смежные классы:

H — подгруппа группы G ; $a \in G$

aH — левый смежный класс группы G по подгр. H ,
порозн. эл-ом a .

Ha — правый см. класс.

Св-ва: 1. $a \in aH$, $a \in Ha$ (H сод-ит единицу)

2. Смежный класс состоит из эл-ов группы G и эл-ов H группы G входит в любой смежный класс.

3. Подгруппа H — и правый и левый смеж. класс, т.е. $eH = He = H$;

4. В любой группе $aH = Ha$
 $\forall a \in G$

Теорема 1 Сметный класс порождается
 $\forall$ своим π -ом.



Д-во: Пои-м, что если $g \in aH$,
 то $aH = gH$

Пусть $g = ah_1$, ($h_1 \in H$)

Тогда: $\forall h \in H$:

$$ah = (ah_1)(h_1^{-1}h) = g h_2 \quad (h_2 = h_1^{-1}h) \Rightarrow$$

$$\Rightarrow aH \subset gH$$

В то же время:

$$gh = a(h_1h) = ah_2 \quad (h_2 = h_1h \in H) \Rightarrow$$

$$\Rightarrow gH \subset aH$$



А значит: $gH = aH$
 (скажем так - для любого)

Теорема 2 Любое $g \in$ сметного класса
 либо совпадает либо не пер-ся.



Д-во:



Если aH и gH имеют общий π -м b , то
 $aH = bH = gH$

Левостороннее (правостороннее) разложение
 группы G по подгр. H - разбиение
 на левое (правое) сметные классы.

3. Нормальное деление.

Опр. Подгр. H группы G наз-ся нормальной дел-м, если $\forall a \in G$
 $aH = Ha$;

Примечание. В абелевой группе $\forall$ подгр. явл-ся нормальным дел-м;

Опр. Эл-ты a и b гр. G наз-ся сопряженными, если $\exists c \in G: a = c^{-1}bc$;

Теорема 3. Подгр. H группы G явл-ся нормальным дел-м $\Leftrightarrow$ она вместе с каждым эл-м содержит все сопряженные с ним эл-ты.

Д-во:

$\Rightarrow$ H - норм. дел., тогда $Hc \subseteq cH$ ($\forall c \in G$)
это означает, что для $\forall h \in H \exists h_1 \in H$:

$$hc = ch_1, \text{ т.е. } c^{-1}hc = h_1 \in H$$

$\Leftarrow$ Возьмем $h \in H, c \in G$, тогда:

$c^{-1}hc \in H$ и $chc^{-1} \in H$, это означает, что $\exists h_1$ и $h_2 \in H: c^{-1}hc = h_1, chc^{-1} = h_2$, или $hc = ch_1, ch = h_2c$ значит:

$$Hc \subseteq cH \text{ и } cH \subseteq Hc \Rightarrow cH = Hc; \blacksquare$$

Фактор группа:

Теорема 4 Служащие классы по норм. дел-ию образуют группу относительно умножения подгр-в группы.

Лемма: Пусть H — норм. делитель группы G . Тогда:

$$\begin{aligned} (aH)(bH) &= \{ \text{из ассоциативности} \} = \\ &= a(bH)H = \{ \text{т.к. } H - \text{норм. делитель} \} = \\ &= a(bH) = abH; \end{aligned}$$

Итак: $(aH)(bH) = (ab)H$

Значит умножение на множестве смежных классов по норм. делителю — ассоциативная операция.

Нейтральный элемент: H , т.к.

$$(aH)H = (aH)(eH) = (ae)H = aH \quad (\forall a \in G)$$

Обратный элемент к классу aH :

класс $a^{-1}H$, т.к.

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H;$$

Опр: Группа смежных классов по норм. делителю — Фактор группа.
 (G/H)

Пример: Вспомогательный: H — подгруппа $\mathbb{Z}$; p — простое число.
 $\mathbb{Z}/H$ состоит из p классов и совпадает с $\mathbb{Z}_p$, т.к. p классов вычетов по модулю p .

Вопрос №10

Изоморфизм групп.

Опр. две группы $G_1^{(*)_1}$ и $G_2^{(*)_2}$ наз-ся изоморфными, если $\exists$ биективное отображение $f: G_1 \rightarrow G_2$, для которого верно:
$$f(a *_1 b) = f(a) *_2 f(b) \quad \forall a, b \in G_1;$$

Обозн: $G_1 \cong G_2$ (f -изоморфизм)

Примеры: 1) $\mathbb{Z} \cong 2\mathbb{Z}$ (четные), т.к. $f(n) = 2n$ - изом.
2) $\langle \mathbb{R}_+, * \rangle \cong \langle \mathbb{R}, + \rangle : f(a) = \ln a$

Св-ва: 1. Отношение изоморфизма явл-ся отношением эквивалентности на мн-ве всех групп.

- Рефлексивно, т.к. $\exists$ тожд. отображение;

- Симметрично, т.к. f -изоморфизм $\Rightarrow f^{-1}$ ($\exists$ в силу биективности) тоже изоморфизм, т.к.:

$$F^{-1}(a' *_2 b') = F^{-1}(f(a) *_2 f(b)) =$$

$\underbrace{f(a)}_{F(a)} \quad \underbrace{f(b)}_{F(b)}$ в силу соответствия f

$$= \{ \text{т.к. } f \text{ - изоморфизм} \} = f^{-1} f(a *_1 b) =$$
$$= a *_1 b = f^{-1}(a') *_1 f^{-1}(b');$$

- Транзитивно, т.к. суперпозиция изоморфизмов также - изоморфизм.

2. В изоморфных группах G_1 и G_2 образ (и прообраз) единицы явл-ся единицей.

Если $a *_1 e = e *_1 a = a$, то
 $f(a) *_2 f(e) = f(e) *_2 f(a) = f(a)$

Значит в силу сюръективности: $f(e) = e'$,
 а в силу инъективности прообраз e' — только;

З. В изоморф. G_1 и G_2 образ (и прообраз)
 обр-ого эл-та эл-та обратного эл-та
 т.е. $f(a^{-1}) = (f(a))^{-1}$;

Обаковы. Аналогично 2.

Теорема 1. (Кэли) Любая конечная
 группа изоморфна нек-ой группе перестановок
 на мн-ве своих эл-ов.



Д-во: $G = \{g_0 = e, g_1, \dots, g_{n-1}\}$ — группа
 n -го пор-ка; Построим отображение φ
 группы G на нек-ое мн-во S
 перестановок мн-ва G , положив
 $\varphi(g) = (g_0g, g_1g, \dots, g_{n-1}g)$ для
 любого $g \in G$.

Так как группа G замкнута относительно
 групповой операции, то $g_0g, g_1g, \dots, g_{n-1}g \in G$

Более того — все эти прообразы различны, т.к.
 из равенств $g_i g = g_j g \Rightarrow g_i = g_j \Rightarrow i = j$;

А значит: $g_0g, g_1g, \dots, g_{n-1}g$ — перестановка
 эл-ов $g_0, g_1, \dots, g_{n-1}$ группы G :

$$\varphi(g) = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-1} \\ g_0g & g_1g & \dots & g_{n-1}g \end{pmatrix}$$

S - нек-ое подмножество симметр. группы всех перест. мн-ва G ;

Покажем, что φ - изоморфизм:

1) φ - инъективно, т.е.

если $g \neq g' (g' \in G)$, то $\varphi(g) \neq \varphi(g')$
 $(g \circ g \neq g' \circ g)$

Т.е. различные эл-ты G соотв. разн. перестановкам из S ;

2) φ - сохраняет групповую операцию, т.е.
 $\varphi(gg') = \begin{pmatrix} g_0 & g_1 & \dots & g_{n-1} \\ g_0(gg') & g_1(gg') & \dots & g_{n-1}(gg') \end{pmatrix}$;

$$\begin{aligned} \varphi(g') \varphi(g) &= \begin{pmatrix} g_0 & \dots & g_i & \dots & g_{n-1} \\ g_0 g' & \dots & g_i g' & \dots & g_{n-1} g' \end{pmatrix} \begin{pmatrix} g_0 & \dots & g_i & \dots & g_{n-1} \\ g_0 g & \dots & g_i g & \dots & g_{n-1} g \end{pmatrix} = \\ &= \begin{pmatrix} g_0 g & \dots & g_i g & \dots & g_{n-1} g \\ (g_0 g') g & \dots & (g_i g') g & \dots & (g_{n-1} g') g \end{pmatrix} \begin{pmatrix} g_0 & \dots & g_i & \dots & g_{n-1} \\ g_0 g & \dots & g_i g & \dots & g_{n-1} g \end{pmatrix} = \\ &= \begin{pmatrix} g_0 & \dots & g_i & \dots & g_{n-1} \\ (g_0 g' g) & \dots & (g_i g' g) & \dots & (g_{n-1} g' g) \end{pmatrix} = \varphi(gg') \end{aligned}$$

3) S - группа, т.е. подгр. группы всех перестановок мн-ва G , т.е. S - изоморфна брз. группе G . 

Теорема 2. Все беск. циклические группы изоморфны аддитивной гр. целых чисел. 

Док-во: G - беск. цик. гр. с обр эл-том a , тогда: $f: a^k \rightarrow k \quad (G \rightarrow \mathbb{Z})$ - изоморфизм. 

Следствие: все бинар. унар. группы изоморфны
между собой

Опр. Изоморфное отображ. группы G
на себя - автоморфизм.
Мн-во всех автоморфизмов группы -
группа относ. суперпозиции отображ.

Вопрос №11.

Гомоморфизм Групп.

Опр. Две гр. G_1 и G_2 с опер. $\ast_1$ и $\ast_2$ наз-ся гомоморфными, если $\exists$ сюръективное

отображение $\varphi: G_1 \rightarrow G_2$:

$$\varphi(a \ast_1 b) = \varphi(a) \ast_2 \varphi(b);$$

φ - гомоморфизм.

Д-во:

В гомоморфных группах:

1) Образом единицы явл-ся единица
($\varphi(e) = e'$) e - ед. G_1 , e' - ед. G_2

2) Образом обр-эл-та явл-ся обр. эл-та
к образу: $\varphi(a^{-1}) = (\varphi(a))^{-1}$;

Пусть φ - гомоморф. $\varphi: G_1 \rightarrow G_2$

Опр. Мно-во $\text{Ker } \varphi = \{a \in G_1 \mid \varphi(a) = e'\}$ -
наз-ся ядром гомоморф. φ .

Теорема 1 Нормальные дел-ли группы и
только они явл-ся ядрами гомоморфизмов
этой группы.

Д-во: $\Leftrightarrow$ Ядро гомоморф. φ □
группы G_1 явл-ся подгруппой G_1 , т.к.
1) если $h_1, h_2 \in \text{Ker } \varphi$, то $\varphi(h_1 \ast_1 h_2) =$
 $= \varphi(h_1) \ast_2 \varphi(h_2) = e' \ast_2 e' = e'$, т.е. $h_1 \ast_1 h_2 \in \text{Ker } \varphi$;
2) если $h \in \text{Ker } \varphi$, то $\varphi(h) = e'$ и
значит: $\varphi(h^{-1}) = (e')^{-1} = e' \Rightarrow h^{-1} \in \text{Ker } \varphi$;

Эта подгр. явл-я нормальным дел-м, т.к. для нее выполнено:

$$\begin{aligned} \text{если } h \in \ker \varphi \text{ и } c \in G, \text{ то} \\ \varphi(c^{-1} * h * c) &= \varphi(c^{-1}) * \varphi(h) * \varphi(c) = \\ &= \varphi(c^{-1}) * e' * \varphi(c) = \varphi(c^{-1} * c) = \\ &= \varphi(e) = e', \text{ т.е.} \end{aligned}$$

$$c^{-1} * h * c \in \ker \varphi;$$

$\Rightarrow$ Пусть H — нормальный дел-м

группы G с операцией $\cdot$, т.е. м., что $\exists$ группа G' и гомоморф. $\varphi: G \rightarrow G'$, ядром которого явл-я H .

В качестве группы G' возьмем фактор-группу G/H

В кач-ве гомоморфизма возьмем отображ. $\varphi: G \rightarrow G/H$: которое $\forall a \in G$ ставит в соот-ие элемент класс aH , т.е. что $\varphi(a) = aH$.

φ — гомоморфизм, т.к.

$$\begin{aligned} \varphi(ab) &= (ab)H = (aH)(bH) = \\ &= \varphi(a) \varphi(b), \quad \forall a, b \in G; \end{aligned}$$

Ядром этого гомоморфизма служит сам нормальный дел-м H .

$\varphi: G \rightarrow G/H$ — естественный гомоморфизм.

Гомоморф $f: G \rightarrow L$ $T = \{f(a) \mid a \in G\}$

T — гомоморфный образ

Вопросы 12, 13. Кольцо. Поле.

Опр. Непустое мн-во K , наделенное двумя ас. операциями $+$ и $\cdot$ наз-ся кольцом, если для $\forall a, b, c \in K$:

- 1) $a + b = b + a$;
- 2) $(a + b) + c = a + (b + c)$;
- 3) $\exists 0 \in K: a + 0 = 0 + a = a$;
- 4) $\forall a \in K \exists -a \in K: a + (-a) = (-a) + a = 0$;
- 5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- 6) $(a + b) \cdot c = a \cdot c + b \cdot c$;
 $a \cdot (b + c) = a \cdot b + a \cdot c$;

Опр. Кольцо наз-ся: 1) коммутативным, если умножение в нем коммутативно

2) кольцом с единицей,

если операция умнож. обладает нейтр. эл-ом

Кольцо явл-ся аддитивной абелевой группой.

Св-ва: 1) Кольцо обл. всеми св-ми аддит. абелев. группы, в частности, в кольце:

а) $\exists! 0$

б) $\forall a: \exists! (-a)$

в) $\forall a, b \in K \exists! x: x + a = b$ $x = \underline{\text{разность } b \text{ и } a}$
($b - a$)

эп-а 2) Опр-ны целые кратные

$n \cdot a = \begin{cases} \underbrace{a + \dots + a}_n, & n > 0; \\ 0, & n = 0; \\ m(-a) = -(ma), & m = -n, n < 0; \end{cases}$

3) В кольце умножение дистриб. относ. сложения

$$a(b - c) = ab - ac; (a - b)c = ac - bc;$$
$$(b = (b - c) + c \text{ и } ab = a(b - c) + ac)$$

3) В кольце для $\forall a: a0 = 0a = 0$
 $a0 = a(b-b) = ab - ab = 0;$

4) В кольце для $\forall a, b: (-a)b = a(-b) = -ab$;
 $a \cdot b + (-a) \cdot b = (a + (-a))b = 0b = 0;$
Сп-вие: $(-a)(-b) = ab, \forall a, b \in K;$

5) В кольце с единицей для $\forall a$:
 $(-1)a = a(-1) = -a;$
 $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0;$

6) В кольце с 1, содержащим не менее $2 \times n$ эл-ов:
 $1 \neq 0$

Если $1 = 0$, то $\exists a \in K: a \neq 0, a \neq 1$.

Тогда из $0 = 1 \Rightarrow 0a = 1a$, т.е. $0 = a$, но $a \neq 0$ (!).

7) В кольце с единицей
 н-во обратных (по умнож.) эл-ов образует
 мультипликативную группу.

Против. обратных эл-ов - обратимо $\Rightarrow$ группоид
 эл-ов алгебр. операций над этим м-во.

Делители нуля:

Д-ль нуля: $a, b \in K, a \neq 0$ и $b \neq 0$, при этом,

$ab = 0$
 левый дел-ль 0 правый дел-ль 0

Подкольцо:

Опр. подкольцом кольца K наз-ся подмн-во F этого кольца, которое само явл-ся кольцом относ. операций, оп-ых в K .
При этом говорят, что кольцо K явл-ся расширением кольца F , а кольцо F вложено в кольцо K .

кольцо $\mathbb{Z}$ - расширение $\mathbb{Z}_{2k}$

кольцо $\mathbb{Z}$ вложено в $\mathbb{Q}$

$$F = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \} - \text{кольцо}$$

F - подкольцо $\mathbb{R}$.

Поле.

Опр. Поле наз-ся коммутативное кольцо с единицей, содержащее не менее двух эл-ов, в котором $\forall a \neq 0 : \exists a^{-1} : a a^{-1} = 1$

Св-ва: 1) Поле обладает всеми св-ми кольца;

2) В поле нет дел-ей: 0,

т.к. если $ab=0, a \neq 0$, то $a^{-1}(ab) = b = 0$

Следствие: умножение явл-ся обратимой операцией ко мн-ке всех отличных от 0 эл-ов поля.

3) В поле P мн-во всех ненулевых эл-ов обр-ет мультипликативную, коммутативную группу и поэтому, в поле:

$$0 \neq 1 \text{ и } 1 \neq 0$$

$$\delta) \forall a \neq 0 : \exists! a^{-1} : aa^{-1} = a^{-1}a = 1,$$

$$\theta) \forall a, b \in P, a \neq 0 \text{ ур-ие}$$

$ax = b$ имеет единственное решение, при этом
 $x = a^{-1}b = ba^{-1}$ этот эл-т

наз-ся частным от дел b на a ,
 (b/a)

4. В поле сокращаются все побочные
 правила обращения с дробями:

$$\text{а)} \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc, \text{ т.ч.}$$

$$b^{-1}a = cd^{-1} \Leftrightarrow b(b^{-1}a)d = b(cd^{-1})d, \text{ т.е.}$$

$$ad = bc$$

$$\delta) \frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}; \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd};$$

$$\theta) \frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b};$$

Расширение поля

Подмно-во F поля P наз-ся подполем
 поля P , если оно само явл-ся полем
 относительно операций, опр-ых в P .
 При этом говорят, что поле P явл-ся
расширением поля F , а F вложено
 в поле P .

поле $\mathbb{R}$ - расширение $\mathbb{Q}$

поле $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ - расширение $\mathbb{Q}$

Теорема 1. Поле рациональных
 чисел вложено в $\forall$ числовое поле.

Док-во:

Пусть P - поле, эл-ты которого



явл-ся числом $a \in R$. Если $a \neq 0$, то R содержит частное $\frac{a}{a}$, т.е. число 1. Складывая число 1 с собой несколько раз, мы получим, что в R содержится все натуральное N . С другой стороны, в поле R должна содержаться разность $n - n$, т.е. число 0, поэтому в поле R найдется и результирующее вычитание $0 - n$, $n \in N$, т.е. все отриц. числа. Наконец, в поле R содержится и частные целых чисел, т.е. вообще все рац. числа.

Хар-ка поля:

Сущ-ют поля, в которых $n \cdot 1 = \underbrace{1 + \dots + 1}_n = 0$

Опр. Наименьшее $n \in N$: $n \cdot 1 = \underbrace{1 + \dots + 1}_n = 0$ наз-ся характеристикой поля.

(Если такого n не сущ-ет, то говорят, что хар-ка равна 0)

Теорема 2. Хар-ой поля может быть либо 0 либо простое число.

Д-во: Пусть n -хар-ка поля и $n = m \cdot k$, $m, k \in N$

$m < n$; $k < n$. Тогда, в силу дистрибутив.:

$$\underbrace{1 + \dots + 1}_n = \underbrace{(1 + \dots + 1)}_m \underbrace{(1 + \dots + 1)}_k = 0 ;$$

Т.к. в поле нет дел-ей нуля, то либо $\underbrace{1 + \dots + 1}_m = 0$ либо $\underbrace{1 + \dots + 1}_k = 0 \Rightarrow$

1 - не намеренное натур. число, обладающее указанным св-вом.

Теорема 3 Если P - поле хар-ки p , то для $\forall$ эл-а $a \in P$ имеет место:

Доказ-во: $pa = 0;$
 $pa = a(p \cdot 1) = a \cdot 0 = 0;$

Изоморфизм колец и полей:

Опр. Два кольца K и K' (два поля P и P') наз-ся изоморфными, если су-ет биективное отображение $\varphi: K \rightarrow K'$ ($\varphi: P \rightarrow P'$), сохр. операции:
 $\forall a, b: \varphi(a + b) = \varphi(a) + \varphi(b); \varphi(ab) = \varphi(a)\varphi(b);$
св-ва:

- 1) Отношение изоморфизма - отнош. эквив. на мн-ве всех колец (полей).
- 2) В изоморфных кольцах (полях):
 - а) образ и прообраз нуля ^{нуль} есть нуль
 - б) образ и прообраз -1 есть -1
 - в) образ и прообраз $a \cdot b$ есть $a \cdot b$ ($\varphi(a)\varphi(b)$)
 - г) образ и прообраз 1 (если она есть) - единица
 - д) образ и прообраз a^{-1} (если она есть) - a^{-1}
- 3) св-во кольца иметь или не иметь дел-ли нуля сохраняется и в изоморфном кольце.

Кольцо, изоморфное полю само явл-ся полем.

Вопрос №14.

Конечно кольцо. Поле конечно по простому модулю.

Рассмотрим аддитивную группу

$\mathbb{Z}_p = \{c_0, c_1, \dots, c_{p-1}\}$ конечно по модулю p .

сложение: $c_m + c_n = c_r \quad r = (m+n) \pmod{p}$;

Ноль: $c_0 \quad (:p)$

противоположный к c_m : $-c_m = \begin{cases} c_0, & m=0; \\ c_{p-m}, & m>0; \end{cases}$

Определим на $\mathbb{Z}_p$ операцию умножения:

св-ва:

$$c_m c_n = c_r \quad r = mn \pmod{p};$$

- 1) $c_m c_n = c_n c_m$; 2) $(c_m c_n) c_k = c_m (c_n c_k)$;
- 3) $\exists e = c_1 : c_m c_1 = c_1 c_m = c_m$ 4) $(c_m + c_n) c_k = c_m c_k + c_n c_k$
- 5) Если p - составное число, то в кольце $\mathbb{Z}_p$ есть делители нуля ($p = mn$) $1 < m < p$; $1 < n < p$,
 $c_m, c_n \in \mathbb{Z}_p$ и $c_m c_n = c_0$

Обоснование св-в:

- 1) Т.к. в таблице входа $mn \pmod{p}$
- 2) т.к. в таблице входа $(mn)k \pmod{p} [m(nk) \pmod{p}]$
... (ассоциативность)

Таким образом, $\mathbb{Z}_p$ - конечно коммутативное кольцо с единицей, которое имеет делители нуля, если p - составное.

$\mathbb{Z}_p$ - конечно кольцо по модулю p .

$$c_m = mH = Hm = \{n \in \mathbb{Z} \mid n \equiv m \pmod{p}\} \quad [H = \{pk \mid k \in \mathbb{Z}\}]$$

$p > 1; p \in \mathbb{N}$

Поле бучетов

Теорема 1. Если p - простое число и $p \geq 2$, то $\mathbb{Z}_p$ - поле хар-ки p .

До-во:

Покажем, что $\mathbb{Z}_p$ - поле. Т.к. $\mathbb{Z}_p$ - коммутативное кольцо с e , то достаточно показать, что для $\forall c_m \in \mathbb{Z}_p$ ($m \neq 0$) существует обратный эл-т.

Рассмотрим преобр. $c_m c_k$ ($k = \overline{0, p-1}$)

Их ровно p и все они различны, т.к:

$$\text{Из того, что } c_m c_k = c_m c_n \quad (k \neq n) \Rightarrow$$

$$\Rightarrow mk \equiv mn \pmod{p} \Leftrightarrow mk - mn : p \Leftrightarrow$$

$$\Leftrightarrow m(k-n) : p \Rightarrow p \text{ составное число}$$

Значит $c_m c_k$ по одному разу проходят все эл-ты мн-ва $\mathbb{Z}_p$, а значит и c_1

$$\text{Учтем } \forall c_m : \exists c_k : c_m c_k = c_1 \Rightarrow$$

$\mathbb{Z}_p$ - поле

Хар-ка этого поля - p , т.к.

$$\underbrace{c_1 + \dots + c_1}_{p \text{ раз}} = c_0, \text{ а } \underbrace{c_1 + \dots + c_1}_m = c_m \neq c_0 \quad (m < p)$$

Теорема 2 Любое поле хар-ки $p \geq 1$ с точностью до изоморфизма явл-ся расширением поля бучетов $\mathbb{Z}_p$.

До-во: В поле, хар-ки p , элементы

натур. 1 (виде $n \cdot 1$, $n = \overline{0, p-1}$) различны.

Эти эл-ты образуют подполе. Оно изомор

ФНО по модулю $\mathbb{Z}_p = \{0, \dots, p-1\}$:
 изоморфизм : $\varphi(n) = c_n \quad (n = \overline{0, p-1})$.

$$(m+1) \cdot (n+1) = \frac{k \cdot p + 1}{p} + t + 1 = t + 1 \quad (t = \overline{0, p-1})$$

$$mn = kp + t \quad (k \in \mathbb{Z})$$

Следствие Любое конечное поле
 явл-ся расширением поля $\mathbb{Z}_p$ (нек-ого
 поля вычетов).

К Вопросу №13.

Теорема 4. В конечном поле
 число эл-ов n имеет вид:
 $n = p^m$ (p - простое, m - натур.)

Док-во:



В конечном поле - поле Хар-ки $p \geq 1$. Т.к.
 1) изоморфное поле одинаковое число
 эл-ов, то достаточно показать, что в
 конечном расширении поля $\mathbb{Z}_p$ содержится.
 $n = p^m$ эл-ов ($m \in \mathbb{N}$, p - простое, т.к. $\mathbb{Z}_p$ - поле).

Теор. 2 Вопрос 14

$F = \{a_0, \dots, a_{k-1}\}$ - расшир. $\mathbb{Z}_p = \{c_0, \dots, c_{p-1}\}$
 F - линейное пр-во над полем $\mathbb{Z}_p$. Пусть
 $e_1, \dots, e_m$ - базис F , тогда F - мн-во
 всевозможных комбинаций:

$$\alpha_1 e_1 + \dots + \alpha_m e_m \quad \alpha_i \in \mathbb{Z}_p \quad i = \overline{1, m}$$

Т.к. у нас есть α_i - р-элемент,
то верно $\exists n$ - об:

$$p^m$$

Вопрос № 15

Линейное пр-во над полем.

Что это в конечном поле,

Пусть дано поле P .

Опр. Непустое мн-во V наз-ся линейным или векторным пр-вом над полем P , если на этом мн-ве определены:

1) Внутрен. закон композиции $V \times V \rightarrow V$
(сложение)

2) Внешний закон композиции $P \times V \rightarrow V$
(умножение на число из поля P)

Удовлетворяющие след. аксиомам ($\forall a, b, c \in V, \forall \alpha, \beta \in P$):

1) $a + b = b + a$;

2) $(a + b) + c = a + (b + c)$;

3) $\exists \theta \in V : a + \theta = \theta + a = a$;

4) $\forall a \in V \exists -a \in V : a + (-a) = (-a) + a = \theta$;

5) $1 \cdot a = a$;

6) $\alpha(\beta a) = (\alpha\beta)a$;

7) $(\alpha + \beta)a = \alpha a + \beta a$;

8) $\alpha(a + b) = \alpha a + \alpha b$;

Линейное пр-во над полем P - векторное,
над полем C - комплексное.

Два в-ре x и y лн. пр-ва наз-ся коллинеарными, если либо $x = \alpha y$ либо $y = \beta x$ ($\alpha, \beta \in P$);

Точки в линейном пр-ве

Опр Аффинным (или точечно-аффинным) пр-вом над линейным пр-вом V наз-ся мн-во S

эт-ов, наз-ых точками, для которого

Задают: а) Лн. пр-во V над полем P ;

б) Отобр. $\cup S \times S \rightarrow V$, ставящее

в соответствие каждой упорядоченной

паре точек $A, B \in S$ вектор $U(A, B) \in V$ и
удовл. следующим аксиомам:

$$1) \text{ Для } \forall m, A \in S \text{ и } \forall b, a \in V \\ \exists! B \in S : U(A, B) = a;$$

$$2) \forall A, B, C \in S :$$

$$U(A, B) + U(B, C) = U(A, C)$$

Размерность аффинного пр-ва S кз-а
размерность лн. пр-ва V .

Примеры: 1. Геом. пр-ва V_1, V_2, V_3 - афф пр-ва
кажд своим собой.

2. $\forall$ лн. пр-во можно считать
аффинным: $\boxed{U: V \times V \rightarrow V: U(a, b) = a - b}$
(кажд своим собой) (1)

3. $\forall$ аффинное пр-во S можно
рассм, как линейное:

Заф-ем точку O - начало $\forall A \in S$ соответ-е
в соотв-е OA - радиус в-р.
лн-во век радиус в-в - линейное
пр-во.

Теорема 1. Обратное

$\varphi: S' \rightarrow V$ ор-ство точек

$$\varphi(A) = \overline{OA}$$

явл-я биекцией, сохраняющей
операцию V линейного пр-ва

$$(2) v(A, B) = v(\varphi(A), \varphi(B));$$

Дока-во:



Биективность отображения φ непосредственно вытекает из аксиомы 1.
на основе (1) ~~равенство~~ (2) $\sim \overline{AB} = \overline{OB} - \overline{OA}$



Вопрос №16.

Понятие комплексных чисел. Комплексная пл-ть.

Опр-ие:

Комплексными числами наз-ся упорядоченные пары (a, b) вещ-ых чисел, для кот-ых понятия рав-ва, суммы, произв. и отлож. с $\mathbb{R}$ вводятся след. об-ом:

1) $(a, b) = (c, d) \Leftrightarrow a = c, b = d;$

2) $(a, b) + (c, d) = (a + c, b + d);$

3) $(a, b) \cdot (c, d) = (ac - bd, bc + ad);$

4) $(a, 0) \in \mathbb{C}$ отлож. с $a \in \mathbb{R}$.

Теорема 1. Мно-во $\mathbb{C}$ всех комплексных чисел явл-ся полем.

Д-во:

Сложение и Умножение - алгебр. операции на $\mathbb{C}$. Они подчиняются всем аксиомам, отдельно стоит отметить: □

$0 = (0, 0); 1 = (1, 0); -z = (-a, -b);$

$z^{-1} = \left(\frac{a}{a^2 + b^2}; -\frac{b}{a^2 + b^2} \right) \quad (z = (a, b) \neq 0);$ ■

Следствие 1. Для $\forall z_1 = (a, b), z_2 = (c, d) \exists! z_3 = z_1 - z_2 = (a - c, b - d);$

Следствие 2. Для $\forall z_1 = (a, b), z_2 = (c, d) \neq 0 \exists! \frac{z_1}{z_2} = \left(\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2} \right);$

Алгебраическая форма комплексного числа:

$$i = (0, 1)$$

$$1) i^2 = (0, 1)(0, 1) = (-1, 0) = -1;$$

2) $\forall z \in \mathbb{C}$ ($z = (a, b)$) представимо в виде:

$$(1) z = a + bi$$

$$(z = (a, b) = (a, 0) + (0, b) = a + (b, 0) \cdot (0, 1) = a + bi)$$

Форма (1) записи комплексного числа наз-ся алгебраической формой числа z , при этом a — действительная часть ($\operatorname{Re} z$), а b — мнимая ($\operatorname{Im} z$).

Если $\operatorname{Re} z = 0$, то z — чисто мнимое число.

Компл. число $\bar{z} = a - bi$ наз-ся сопряженным к числу $z = a + bi$.

Теорема 2 Операция сопряж. компл-ого числа обладает следующими св-ми:

$$1) \bar{\bar{z}} = z; \quad 4) \bar{z}z = a^2 + b^2 \quad \forall z = a + bi;$$

$$2) z = \bar{z} \Leftrightarrow z \in \mathbb{R}; \quad 5) \overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2;$$

$$3) z + \bar{z} = 2a \quad \forall z = a + bi; \quad \overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2;$$

$$(\overline{z_1 / z_2}) = \bar{z}_1 / \bar{z}_2; \quad z_2 \neq 0$$

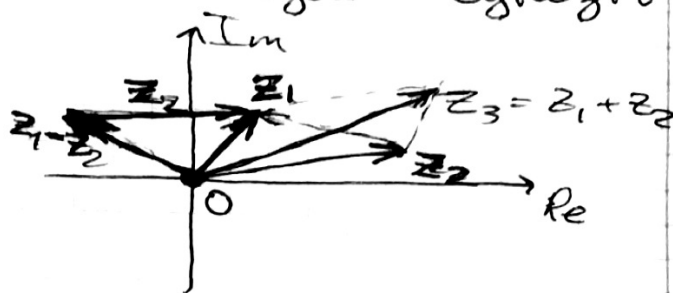
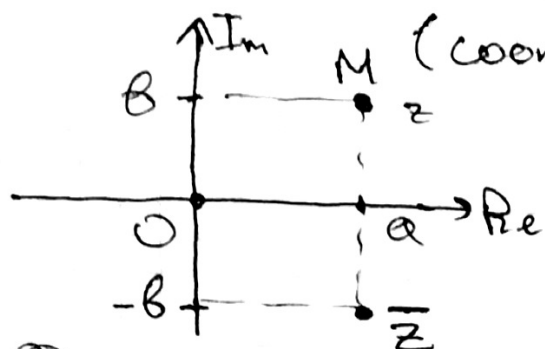
 Зам. Св-ва пров-ся нею представимо, исходя из орг-ца.

Замечание:

В алгебр. форме удобно производить вычисл. (с учетом $i^2 = -1$) аналогично вычисл. в $\mathbb{R}$.

Комплексная пл-ть. Пусть задана ^{прямоуг.} декартова с.и.

Поставим $\forall z \in \mathbb{C} \quad z = a + bi$ в соотв-ие точку $M(a, b)$



Опр. Пл-ть, точками которой изобр. комп-ое числа - комп-ая пл-ть, ось абсцисс - вещ-ая ось, а ось ординат - мнимая ось (Ox , Oy)

На коорд. пл-ти удобно иллюстр. сложение и вычит. комп. чисел:

$\mathbb{C}$ по модулю радиус - векторов соотв-х точек.

Дополнительно:

I. Сопряженная матриц.: $A = (a_{ij}) \in \mathbb{C}^{m \times n}$

Опр. Матрица $A^H = (a^h_{ij}) \in \mathbb{C}^{n \times m}$ наз-ся сопряженной к матрице A , если:

$$a^h_{ij} = \overline{a_{ji}} \quad i = \overline{1, n}, \quad j = \overline{1, m};$$

Св-ва:

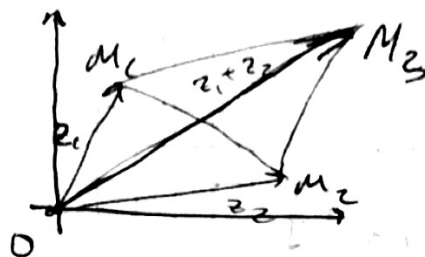
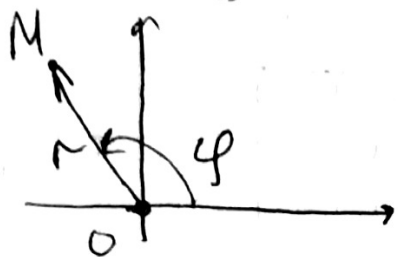
- 1) $(A+B)^H = A^H + B^H$; 4) $(A^H)^H = A$;
- 2) $(\alpha A)^H = \overline{\alpha} A^H; \forall \alpha \in \mathbb{C}$; 5) $\det A^H = \overline{\det A}$;
- 3) $(AB)^H = B^H A^H$; 6) $\text{rg } A^H = \text{rg } A$;

II Другое представление комп. чисел.:

$$\mathbb{C}' = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

$$\mathbb{C}' \cong \mathbb{C} \quad \varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix};$$

Вопрос № 17. Тригонометрич. форма
комплексного числа. Модуль и аргумент
произвед. комп. чисел.



Положение точки на пл-ти однозначно опре-
 ся её полярными коорд., т.е.
 расстоянием r до н. коорд. и углом φ
 между r и полож. направл. оси абсцисс (Ox)

Опр. Модуль комплексного числа
 $z = a + bi$ наз-ся числом $r = \sqrt{a^2 + b^2}$;

Обозн: $|z|$

св-ва:

- 1) $|z| \in \mathbb{R}, |z| \geq 0$
- 2) $|z| = 0 \Leftrightarrow z = 0$;
- 3) $|z|$ — полярный радиус r ;
- 3) $|z| = \sqrt{z \bar{z}}$;
- 4) $z \in \mathbb{R} \Rightarrow |z|$ совпадает с абсц. вел. z .

Опр. Аргумент комплексного числа $z \neq 0$
 наз-ся углом φ (между r и полож. направл. Ox).

св-ва: $\varphi = \arg z$

- 1) $\arg z$ не опр-на для $z = 0$,
- а для $z \neq 0$ опр-на с точностью до $2\pi k$
 $k \in \mathbb{Z}$.

2) арг z определяется от φ тем, что имеет бесконечно много значений, т.е.:

$$\arg z = \varphi + 2\pi k; k \in \mathbb{Z};$$

при этом $\varphi \in [0, 2\pi)$

$$3) z_1 = z_2 \Leftrightarrow \begin{cases} |z_1| = |z_2| \\ \arg z_1 = \arg z_2 + 2\pi k, |z_1| \neq 0 \end{cases}$$

Теорема 1.

Любое комплексное число $z \neq 0$ может быть записано в виде:

$$z = r(\cos \varphi + i \sin \varphi);$$

$$[\text{где } r = |z|; \varphi = \arg z]$$

Доказ. $z = a + bi$

Для полярн. коорд.: $a = r \cos \varphi$
 $b = r \sin \varphi$

и т.о. : $z = r(\cos \varphi + i \sin \varphi)$

Тригонометр. форма записи.

Теорема 2.

Для $\forall z_1, z_2 \in \mathbb{C}$ справедливо:

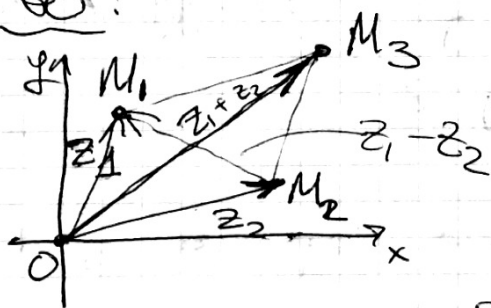
$$(*) \quad ||z_1| - |z_2|| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|$$

Доказ.

Нер-ба А-на



$$\begin{aligned} b &\leq a + c \\ c &\leq a + b \\ a &\leq b + c \end{aligned}$$



1) (*) вытекает из нер-ба А-на

($\triangle OM_2M_3, OM_1, M_2$)

2) Если O, M_1, M_2 лежат

на одной прямой в (*) будут только нулевые нер-ва, а их

проверка м.д. осуществлена перебором
в-ов расположения этих точек.

(*) - Нерва д-на на комп-ой пл-ти;

Теорема 3. При умнож. комп. чисел
их модули умнож., аргументы складываются
При делении: модули делятся, аргументы
вычитаются.

$$|z_1 z_2| = |z_1| \cdot |z_2|; \quad \arg z_1 z_2 = \arg z_1 + \arg z_2;$$

$$|z_1 / z_2| = |z_1| / |z_2|; \quad \arg \frac{z_1}{z_2} = \arg z_1 - \arg z_2;$$

Доказ-во: $z_k = r_k (\cos \varphi_k + i \sin \varphi_k) \quad k=1,2;$

$$\begin{aligned} 1) z_1 z_2 &= r_1 r_2 (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2 + \\ &+ i [\sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2]) = \\ &= r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)); \end{aligned}$$

2) Если $z_2 \neq 0$, то

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} \cdot \frac{(\cos \varphi_1 + i \sin \varphi_1)}{(\cos \varphi_2 + i \sin \varphi_2)} \cdot \frac{\cos \varphi_2 - i \sin \varphi_2}{\cos \varphi_2 - i \sin \varphi_2} =$$

$$= \frac{r_1}{r_2} \cdot (\cos \varphi_1 \cos \varphi_2 + \sin \varphi_1 \sin \varphi_2 + i (\sin \varphi_1 \cos \varphi_2 - \cos \varphi_1 \sin \varphi_2))$$

$$= \frac{r_1}{r_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2));$$

Замечание 1 Если $\begin{bmatrix} z_1=0 \\ z_2=0 \end{bmatrix}$ то Тер 3 опуск.
только к модулям.

Замечание 2 Теорема 3 справедлива для
в-на комплексных.

Вопросы 18, 19.

Возв. в степень, извлечение корня. Формула Муавра.

I. Возв. в степень

Опр. Пусть $n \in \mathbb{Z}$ и $z \in \mathbb{C}$. Число z^n , опр-ая
рав-ии $z^n = \underbrace{z \cdot \dots \cdot z}_n$ при $n \in \mathbb{N}$ и $z^n = 1$ ($n=0$)
 $z^n = 1/z^m$ ($m = -n \in \mathbb{N}$) кас-ая $z \neq 0$
степенью числа z .

Муавра
Формула Теорема 1. Если $z = r(\cos \varphi + i \sin \varphi)$, $n \in \mathbb{Z}$,
то

$$z^n = r^n (\cos n\varphi + i \sin n\varphi);$$

До-во: Для $n \in \mathbb{N}$ рав-во вытекает $\square$

из опред. произв. комплексных чисел
в тригонометр. форме. Для $n=0$ р-на следует
из опред. $z^0 = 1 = r^0 (\cos 0 + i \sin 0)$. Если $n < 0$
и $n = -m$, $m \in \mathbb{N}$, то:

$$\begin{aligned} z^n &= \frac{1}{z^m} = \frac{1}{r^m (\cos m\varphi + i \sin m\varphi)} = r^n (\cos(m\varphi) - i \sin(m\varphi)) \\ &= r^n (\cos n\varphi + i \sin n\varphi) \end{aligned}$$

Извлечение корня

Опр. Пусть $n \in \mathbb{N}$. Корни n -ой степени
из $z \in \mathbb{C}$ кас-ая число $a \in \mathbb{C}$: $a^n = z$
[Если $z=0$, то $a=0$]

Теорема 2 Для ненулевого $z = r(\cos \varphi + i \sin \varphi)$ существуют ровно n различных корней $\alpha_1, \dots, \alpha_n$ n -й степени:

$$\alpha_k = \sqrt[n]{r} \cdot \left(\cos \frac{\varphi + 2\pi k}{n} + i \sin \frac{\varphi + 2\pi k}{n} \right);$$

$$k = \overline{0, n-1}$$

□ Доказ. Пусть α — корень n -й степени из z и $\alpha = r(\cos \Theta + i \sin \Theta)$. Тогда $\alpha^n = z$

$$\text{Умно } r^n (\cos n\Theta + i \sin n\Theta) = r(\cos \varphi + i \sin \varphi);$$

$$\text{А значит: } r^n = r; n\Theta = \varphi + 2\pi k; k \in \mathbb{Z};$$

Т.к. $r > 0$ и $r > 0$ то $\sqrt[n]{r}$ — единств. $\Rightarrow \alpha$ есть-я корнем n -ой ст. из $z \Leftrightarrow \varphi = \varphi + 2\pi k; \Theta = \frac{\varphi + 2\pi k}{n}; k \in \mathbb{Z}$

$$\text{Т.е. числа } \alpha_k = \sqrt[n]{r} \left(\cos \frac{\varphi + 2\pi k}{n} + i \sin \frac{\varphi + 2\pi k}{n} \right); k \in \mathbb{Z}$$

и только они есть-я корнями n -ой ст. из z

Числа α_k ($k = \overline{0, n-1}$) — различны, т.к. окружность самое большое на $\frac{2\pi(n-1)}{n} < 2\pi$, а при $k \geq n$ — совпадают с одними из $\alpha_0, \dots, \alpha_{n-1}$

Т.к. если $k = nq + r$ $0 \leq r \leq n-1$, то

$$\frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2\pi r}{n} + 2\pi q; q \in \mathbb{Z}$$

$$\text{и } \alpha_k = \alpha_r$$

Геометрическая интерпретация корней:

На комплексной n -ми все корни n -й степени из ненулевого числа z расположены на окруж-ти ($r = \sqrt[n]{|z|}$) и делят эту окруж-ть на n равных частей, т.к. $\arg \alpha_k = \arg \alpha_{k-1} + \frac{2\pi}{n}$.

Две корткей из 1.:

$$\varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}; \quad k = \overline{0, n-1};$$

Они расположены на ед. окр-ти и делят её на n равных частей, начиная с $\varepsilon_0 = 1$

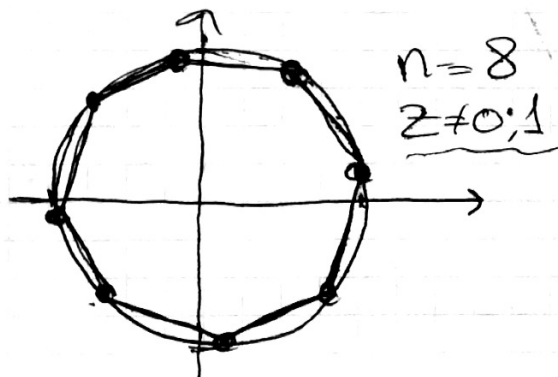
При этом действительных корткей м.б. либо 2 (n - чётно): ε_0 и $\varepsilon_{n/2}$ либо один, если (n - нечётно): ε_0 .

В $\forall$ случае мнимых (не действ.) корткей всегда чётное число и они расположены симметрично относительно действительной оси (т.е. попарно сопряжённые).

Теорема 3. Все корткы n -ой степени из $z \neq 0, z \in \mathbb{C}$ получаются умножением одного из них на все корткы n -ой ст. из 1.

Д-во: $\alpha_k, k = \overline{0, n-1}$ - корткы n -ой степени из $z = r(\cos \varphi + i \sin \varphi)$, окр-ые мы ум-но в Теор. 2. □

Тогда: $\alpha_k \varepsilon_0 = \alpha_k; \alpha_k \varepsilon_1 = \alpha_{k+1}, \dots, \alpha_k \varepsilon_{n-k} = \alpha_0, \dots, \alpha_k \varepsilon_{n-1} = \alpha_{k-1}$ ■



Вопрос №20

Группа корней n -ой степени из единицы.
Первообразные корни.

I. Группа корней n -ой степени из единицы.

Рассм. мн-во $\mu_n = \{ \epsilon_0, \epsilon_1, \dots, \epsilon_{n-1} \}$ всех корней n -ой ст. из 1

1. μ_n - абелева мультипликативная группа, как подгруппа мультипликативной группы ненулевых компл. чисел.

2. μ_n - циклическая группа, порожденная ϵ_1 , т.е. $\epsilon_k = \epsilon_1^k$; (сочетание циклич.)

Этой группой исчерпываются все группы кор-на n .

Теорема 1.

Все цикл. группы кор-на n изоморфны мул-т. группе корней n -ой степени из единицы.

Д-во. α - обр-ий эл-т цикл. гр. G □
Каждому $\alpha^k \in G$ ($0 \leq k < n$) поставим в соответствие ϵ_k (корень n -ой ст. из 1). Это будет взаимно однозначное отображение гр. G на мул-т-ую гр. μ_n корней n -ой ст. из 1 ■

II. Первообразные корни.

Опр. Корень ϵ_k наз-ся первообразным корнем n -ой степени из 1, если он не явл. корнем из единицы никакой меньшей чем n степени.

Для любого $n \geq 2$ ε_1 - первообр. корень
 для $n=4$: $\mu_4 = \{1, i, -1, -i\}$, $\varepsilon_3 = -i$ - не
 первообр.

Теорема 2. Корень n -ой степени из единицы
 явл. первообр. корнем $\Leftrightarrow$ его степени ε^k $k=0, n-1$
 различны.

□ До-во: $\Rightarrow$ Пусть $\varepsilon^k = \varepsilon^l$ при $0 \leq k < l < n-1$

тогда $\varepsilon^{l-k} = 1$, $1 \leq l-k \leq n-1 \Rightarrow \varepsilon$ явл-я
 корнем из 1 степени, меньшей чем n .

$\Leftarrow$ Пусть ε - не первообразный корень.
 Тогда $\exists k < n$: $\varepsilon^k = 1 = \varepsilon^0$ и степени

■ $\varepsilon^0, \varepsilon^1, \dots, \varepsilon^{n-1}$ не будут различны(?!).

Следствие 1: Корень ε n -ой степени, из 1
 явл-я первообразным корнем $\Leftrightarrow$ он является
 образующим ~~цикл.~~ циклич. группой H всех корней
 n -ой степени из 1.

Следствие 2 Корень $\varepsilon_k \in H$ n -ой степени
 из 1 явл-я первообразным $\Leftrightarrow k$ и n взаимно
 просты (на осн. теор. об образующей n -е
 циклич. группы)

Вопрос №21

Концы многочленов. Степени с остатком.

Опр Многочленом n -й ^{степени} от пер. ой x над полем P наз-я выражение вида:

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

где $a_i \in P \forall i, a_n \neq 0$.

$0 \in P$ — нулевой многочлен ($\in 0$ коэфф.)

$$f(x) = \sum_{k=0}^n a_k x^k \in P[x]; \deg f = n;$$

Опр Два многочлена наз-я равными, если

$$\text{для } f(x) = \sum_{k=0}^n a_k x^k \text{ и } g(x) = \sum_{k=0}^s b_k x^k:$$

$$\deg f = \deg g = n; a_i = b_i \quad i = \overline{0, n};$$

Опр. Суммой многочленов f и g наз-я многочлен:

$$h(x) = \sum_{i=0}^{\max(n,s)} (a_i + b_i) x^i;$$

(недостающие зам. 0)

Опр Произведением многочленов f и g наз-я

многочлен $h(x) = \sum_{k=0}^{n+s} c_k x^k$, где $c_k = \sum_{\substack{i+j=k}} a_i b_j$

все возможные i, j : $i+j=k$
 $k = \overline{0, n+s};$

Св-ва:

1. Для $\forall f(x) \in P[x]: 0 + f(x) = f(x) + 0 = f(x);$
2. Для не нулевых $f, g \in P[x] \quad \deg f + g \leq \max(\deg f, \deg g);$
3. Если $f, g \in P[x]$, то $(f+g) \in P[x]$, т.е. множество — замкн. операц. на $P[x]$
4. $\deg fg = \deg f + \deg g$ (произведение ненулевых многочленов не может быть нулевым).

5. Если $f, g \in R[x]$, то $fg \in R[x]$, т.е. умнож. - ассоциатив. операция на $R[x]$.

6. $\mathcal{L}f(x) = \sum_{k=0}^n \mathcal{L}a_k x^k$ - Внешний закон композиции для $R[x]$.

Теорема 1 Мно-во $R[x]$ всех многочленов над полем R явл-ся коммутативным кольцом с единицей и без дел-ей нуля.

□ До-во: Проверим все аксиомы кольца

$R[x]$ - аддитивная абелева группа:

- Коммут. и ассоциативн. - очевидно;
- $0: f(x) \equiv 0$;
- $-f: + \sum_{k=0}^n (-a_k) x^k$;
- Коммутативность ~~умнож.~~ сред. из след;
- Ассоциативность умножения

$$f_n(x) = \sum_{k=0}^n a_k x^k; \quad g_s(x) = \sum_{k=0}^s b_k x^k; \quad h_p(x) = \sum_{k=0}^p c_k x^k;$$

Обозначим через $\alpha_k, \beta_k, \gamma_k$ и δ_k коэф. у x_k в многочл:

$$f(x)g(x), \quad g(x)h(x), \quad (f(x)g(x))h(x) \text{ и } f(x)(g(x)h(x)),$$

Тогда:

$$\gamma_k = \sum_{i+j=k} \alpha_i c_j = \sum_{i+j=k} \left(\sum_{r+t=i} a_r b_t \right) c_j =$$

$$= \sum_{r+t+j=k} a_r b_t c_j$$

$$\delta_k = \sum_{r+i=k} a_r \beta_i = \sum_{r+i=k} a_r \left(\sum_{t+j=i} b_t c_j \right) =$$

$$= \sum_{t+j+r=k} a_r b_t c_j$$

т.е. $\gamma_k = \delta_k$, а значит, т.к.

$$\deg(fg)h = \deg f(gh) = n+s+p \quad \text{Выводим:}$$

$$(fg)h = f(gh)$$

• Поле аддитивной группы. идеал $f(x) \equiv 1$;

• Дистрибутивность

$$\sum_{i+j=k} (a_i + b_i) c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j$$

$$(F + G)h = Fh + Gh;$$

• На основе леммы 4 в $P[x]$ нет дел. 0;

Следствие Мно-во $P[x]$ абн-а мин. пр-вом над полем P .

Замечание $P[x]$ не абн. полем, т.к. не у всякого многочлена есть обр-ый (т.е. $FF^{-1} = 1$ выполнено только для $F: \deg F = 0$).

Деление многочленов

Теорема 2. Для $\forall$ мн-ов $f(x)$ и $g(x) \in P[x]$, где $g(x) \neq 0$ $\exists!$ $q(x)$ и $r(x) \in P[x]$:

$$f(x) = g(x) \cdot q(x) + r(x)$$

$$\text{где: } \begin{cases} \deg r < \deg g; \\ r = 0; \end{cases}$$

До-во: 1) $f(x) \neq 0$ (иначе $q(x) = r(x) = 0$). □

$$f(x) = \sum_{k=0}^n a_k x^k; \quad g(x) = \sum_{k=0}^s b_k x^k; \quad n \geq s$$

(иначе $q(x) = 0; r(x) = f(x)$)

1. Пусть $n = 0$ тогда $s = 0$ и $q(x) = a_0 b_0^{-1}; r(x) = 0$;

2. Пусть верно для $\forall$ многочлена степени меньше n . Док-м для $f(x)$ степени $n \geq s$;

Построим остаток $\frac{a_n}{b_s} x^{n-s}$ (нужно убрать старшую степень) и составим разность $f_1(x) = f(x) - \frac{a_n}{b_s} x^{n-s} g(x)$

Дано: $\begin{cases} f_1(x) = 0; \\ \deg f_1 < n; \end{cases} \Rightarrow \begin{cases} q(x) = \frac{a_n}{b_s} x^{n-s}; r(x) = 0; \end{cases} \quad (1)$

① по алгоритму деления $f_1(x)$

$\sim(x) : f_1(x) = g(x) q_1(x) + r(x), \text{ где:}$

$\begin{cases} r(x) = 0; \\ \deg r < \deg g \end{cases} \Rightarrow f(x) = \frac{a_n}{b_s} x^{n-s} g(x) +$

$+ g(x) q_1(x) + r(x)$

Поэтому $q(x) = \frac{a_n}{b_s} x^{n-s} + q_1(x)$ и получим:

$f(x) = q(x) g(x) + r(x);$

2) Дано уравнение:

Пусть $q_1(x), r_1(x) \in P[x]$ такие, что выполняются, т.е.

$f(x) = q(x) g(x) + r(x) = q_1(x) g(x) + r_1(x), \text{ т.е.}$

$g(x)(q(x) - q_1(x)) = r_1(x) - r(x);$

Если $r_1(x) - r(x) \neq 0$ то и $q_1(x) - q(x) \neq 0$

при этом $\deg(r_1(x) - r(x)) < S$, а $\deg g(x)(q(x) - q_1(x)) \geq S \quad (?!)$ $\Rightarrow$

$\Rightarrow r_1(x) = r(x)$, но, т.к. $\notin P[x]$ не делит 0, то и $q_1(x) = q(x)$, получим:

$r(x) = r_1(x)$ и $q(x) = q_1(x);$

Вопрос №22. НОД по д-в. Алгоритм Евклида.

Определение: $f(x) = q(x)g(x) + r(x)$

• $q(x)$ — частное (неполное); • $r(x)$ — остаток

• $r(x) = 0 \Rightarrow f(x)$ делится на $g(x)$ и $g(x)$ — делитель $f(x)$

• Многочлен $q(x)$ наз-ся общим дел-ем $f(x)$ и $g(x)$, если он явл-ся дел-ем каждого из них.

• Многочлены не имеющие никаких общих дел-ей, кроме многочленов нулевой степени — взаимно простые.

• $d(x)$ называется наиб. общим дел-ем $f(x)$ и $g(x)$ (ненулевым), если:

(1) $d(x)$ — общий дел-ем $f(x)$ и $g(x)$

(2) $d(x)$ — делится на $\forall$ другой общий дел-ем $f(x)$ и $g(x)$

$$\alpha d(x) = \text{НОД}(f(x), g(x)); \forall \alpha \in \mathbb{R} (\neq 0);$$

Теорема 1

Для $\forall$ ненулевой пары многочленов $f(x) \neq 0$ и $g(x) \neq 0 \in \mathbb{R}[x]$ $\exists$ НОД $(f(x), g(x))$, Он определ-ся однозначно с точностью до множителя нулевой степени.

Доказ-во: Алгоритм построения

НОД (f, g) наз-ся: Алгоритм Евклида

1) Выполним цепочку делений с остатком:

$$\begin{aligned}
 f(x) &= g(x) q_1(x) + r_1(x) & \deg r_1(x) < \deg g(x) \\
 g(x) &= r_1(x) q_2(x) + r_2(x) & \deg r_2(x) < \deg r_1(x) \\
 r_1(x) &= r_2(x) q_3(x) + r_3(x) & \deg r_3(x) < \deg r_2(x) \\
 (*) \quad \left\{ \begin{aligned}
 r_{k-3}(x) &= r_{k-2}(x) q_{k-1}(x) + r_k(x); \deg r_{k-1} < \deg r_{k-2} \\
 r_{k-2}(x) &= r_{k-1}(x) q_k(x) + r_k(x); \deg r_k < \deg r_{k-1} \\
 r_{k-1}(x) &= r_k(x) q_{k+1}(x);
 \end{aligned} \right.
 \end{aligned}$$

- Степени остатков уменьшаются и процесс завершится в тот момент, когда выполнится деление на 0.
- Пусть $r_k(x)$ — последний ненулевой остаток.

■ Пока-м, что $r_k = \text{НОД}(f, g)$:

- Проходя по р-м (*) снизу вверх, легко установить, что $r_k(x)$ явл-я ген-м $r_{k-1}, r_{k-2}, \dots, r_1(x), g(x), f(x)$, т.е. общим ген-м $f(x)$ и $g(x)$.

- Проходя по р-м (*) сверху вниз можно установить, что все остатки $r_1(x), r_2(x), \dots, r_k(x)$ ген-а на $\forall$ общий ген-м $f(x)$ и $g(x)$.

2) Пусть $d_1(x) = \text{НОД}(f, g)$ и $d_2(x) = \text{НОД}(f, g)$
Тогда согласно определению:

$$d_1(x) = d_2(x) q_1(x) \text{ и } d_2(x) = q_2(x) d_1(x)$$

$$\text{и } \deg d_1 \geq \deg d_2, \text{ а } \deg d_2 \geq \deg d_1 \Rightarrow$$

$$\Rightarrow \deg d_2 = \deg d_1 \text{ и } d_1(x) \text{ делится}$$

на $d_2(x)$ только на множители нулевой степени.

Вопросы № 23, № 24.

Значения многочлена и корни.

Теорема Безу.

Многочлены или формальные выражения или Φ -цм. Значениями двух операций равенства.

Многочлен $f(x)$ можно рассматривать и как Φ -цм от пер-ой x . Если $f(x) = \sum_{k=0}^n a_k x^k$ - многочлен над полем P , c - число из поля P , то число $F(c) = \sum_{k=0}^n a_k c^k$ наз-ся значением многочлена $f(x)$ при $x=c$.

Из теории Φ -цм известно, что две Φ -цм наз-ся равными, если их значения равны при всех зн-ях пер-ой.

Значит опер-ия арифм. операций для многочленов остаются в силе:

Если $\varphi(x) = f(x) + g(x)$; $\psi(x) = f(x)g(x)$, то $\varphi(c) = f(c) + g(c)$ и $\psi(c) = f(c)g(c) \forall c \in P$.

Опр. Корнем многочлена $f(x) \in P[x]$ наз-ся число $c \in P$, такое что $f(c) = 0$.

Теорема 1. (Безу)

Остаток от дел-ия многочлена $f(x)$ на $(x-c)$ равен $f(c)$.

Док-во:

$$f(x) = (x-c)q(x) + r(x)$$

($\deg r < \deg(x-c) = 1$), т.е. $r(x) = b$ - константа.

Рассматривая значения обеих частей этого рав-ва при $x=c$ получим: $f(c) = f(c)$

Следствие. Число $c \in P$ является корнем многочлена $f(x) \in P[x] \Leftrightarrow$ многочлен $f(x)$ делится на $x - c$ в кольце $P[x]$.

Теорема 2 (эвал. 2-х стр-ий рав-ва)

Если два многочлена $f(z), g(z) \in C[z]$ степени которых не превосходят $n \geq 1$, имеют равные значения при более чем n различных значениях пер-ой, то они равны.

□

Д-во:

Многочлен $h(z) = f(z) - g(z) \in C[z]$ имеет

более n различных корней, но $\deg h(z) \leq n$, поэтому $h(z) = 0$.

Следствие 1. Два многочлена $f(z), g(z) \in C[z]$ равны $\Leftrightarrow$ совпадают их значения при всех $n+1$ пер-ой z .

Следствие 2. $f(z) \in C[z]$ степени $n \geq 1$ однозначно стр-ся своими значениями в $n+1$ различных точках.

• Если $f(z)$ в м. $\alpha_1, \dots, \alpha_{n+1}$ ($\alpha_i \neq \alpha_j$ при $i \neq j$) принимает значения $f(\alpha_1), \dots, f(\alpha_{n+1})$, то

$$f(z) = \sum_{k=0}^{n+1} f(\alpha_k) \frac{(z - \alpha_1) \dots (z - \alpha_{k-1})(z - \alpha_{k+1}) \dots (z - \alpha_{n+1})}{(\alpha_k - \alpha_1) \dots (\alpha_k - \alpha_{k-1})(\alpha_k - \alpha_{k+1}) \dots (\alpha_k - \alpha_{n+1})}$$

Интерполяционный многочлен Лагранжа →

Вопрос № 25.

Основная теорема Алгебры.

Разложение многочлена на линейные
множители.

I. Алгебр. замкнутость поля $\mathbb{C}$.

Опр. Поле P наз-ся алгебраически замкнутым, если $\forall$ многочлен $f(x) \in P[x]$ степени $n \geq 1$ обр-ет в P хотя бы один корень.

Замечание: Очевидно, что поле действительных чисел $\mathbb{R}$ не явл. алгебр. замкнутым, т.к. $x^2 + 1$ не имеет действ. корней.

Теорема 1. (основная теор. Алгебры)

Поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Для док-ва требуется рассмотреть ряд вспомогательных лемм:

$$f(z) = a_0 + a_1 z + \dots + a_n z^n \in \mathbb{C}[z]$$

Лемма 1. Пусть $f(z) = a_1 z + \dots + a_n z^n \in \mathbb{C}[z]$ - многочлен с ненулевыми свободными членами. Тогда $\forall \varepsilon > 0$ $\exists \delta > 0$: для $\forall z : |z| < \delta$ выполняется:

$$|f(z)| < \varepsilon;$$

Д-во: Пусть $|z| < 1$, тогда:

$$|f(z)| = |z| \cdot |a_1 + a_2 z + \dots + a_n z^{n-1}| \leq$$

$$\leq |z| \cdot (|a_1| + \dots + |a_n|)$$

Пусть $M = \min(1, \frac{\varepsilon}{M})$

Тогда $\forall z : |z| < \delta$ выполняется $|f(z)| \leq |z| \cdot M < \frac{\varepsilon}{M} \cdot M = \varepsilon$

Опр. Комплексная φ -чис $f(z)$ ($z \in \mathbb{C}$) наз-ся непр-ной

в точке z_0 , если $\forall \varepsilon > 0 \exists \delta > 0$:
для $\forall z: |z - z_0| < \delta$ выполняется $|f(z) - f(z_0)| < \varepsilon$,

Лемма 2 Многочлен $f(z)$ есть непр-ая
 φ -чис во всех точках комплексной п-ти.

Δ Доказ. $z_0 \in \mathbb{C}$; Разложим $f(z)$ по степеням
 $z - z_0$:

$$f(z) = c_0 + c_1(z - z_0) + c_2(z - z_0)^2 + \dots + c_n(z - z_0)^n;$$

Тогда $c_0 = f(z_0)$, так что

$$f(z) - f(z_0) = c_1(z - z_0) + \dots + c_n(z - z_0)^n,$$

$g(z - z_0) = c_1(z - z_0) + \dots + c_n(z - z_0)^n$ - многочлен
от $z - z_0$ с нулевым своб. членом, а
значим по Лемме 1:

$\forall \varepsilon > 0 \exists \delta > 0$: для $\forall z: |z - z_0| < \delta$ выполняется:

$$|g(z - z_0)| < \varepsilon, \text{ то}$$

$$|f(z) - f(z_0)| = |g(z - z_0)| < \varepsilon;$$

Лемма 3. Модуль многочлена есть непр-ная

φ -чис.

Δ Доказ. $|f(z) - f(z_0)| \geq ||f(z)| - |f(z_0)||$,

а для $|f(z) - f(z_0)|$ известно: $\forall \varepsilon > 0 \exists \delta$:

$$\text{для } \forall z: |z - z_0| < \delta: |f(z) - f(z_0)| < \varepsilon \Rightarrow$$

$$\Rightarrow \underline{|f(z)| - |f(z_0)|} < \varepsilon$$

Лемма 4 Если $f(z)$ — многочлен степени $n \geq 1$,
то для $\forall M > 0 \exists R > 0$: для $\forall z: |z| > R$, верно
 $|f(z)| > M$.

До-каз.

Δ

Запишем $f(z)$ в виде:

$$f(z) = a_n z^n \left(1 + \frac{a_{n-1}}{a_n} z^{-1} + \dots + \frac{a_0}{a_n} z^{-n} \right) =$$

$$= a_n z^n (1 + g(z^{-1}));$$

где $g(z^{-1})$ — многочлен от z^{-1} с нулевым
своб. членом. В силу Леммы 1 для $\varepsilon = \frac{1}{2} \exists \delta > 0$:
при $|z^{-1}| < \delta$ верно:

$$|g(z^{-1})| < \frac{1}{2}$$

Многочлен $a_n z^n$ м.б. сколь угодно
большим, именно при $|z| > \sqrt{2M/|a_n|}$
будем $|a_n z^n| > 2M$.

Тогда пусть $R = \max\left(\sqrt{\frac{2M}{|a_n|}}, \frac{1}{\delta}\right)$.

Тогда, если $|z| > R$, то $|z^{-1}| < \delta$ и
 $|z| > \sqrt{2M/|a_n|}$, а значит:

$$|f(z)| = |a_n z^n| \cdot |1 + g(z^{-1})| \geq$$

$$\geq |a_n z^n| \cdot |1 - |g(z^{-1})|| > 2M(1 - \frac{1}{2}) = M. \blacktriangle$$

Опр. Число $z_0 = x_0 + iy_0$ наз-а пределом
послед-ств $z_n = x_n + iy_n$, если:

$\forall \varepsilon > 0 \exists N \in \mathbb{N}$: для $\forall n \geq N$ $|z_n - z_0| < \varepsilon$

$$\lim_{n \rightarrow \infty} z_n = z_0 \Leftrightarrow \lim_{n \rightarrow \infty} x_n = x_0 \text{ и } \lim_{n \rightarrow \infty} y_n = y_0.$$

Опр. Послед-ство z_n наз-а ограниченной,
если $\exists R > 0: |z_n| \leq R \quad (\forall n)$

Лемма 5 Из любой отр. рас-ти z_n можно выбрать с.с.с. подрас-тв.

Δ Д-во. Пусть $z_n = x_n + iy_n$ и $|z_n| \leq R$

Тогда $|x_n| \leq R$, так что x_n - отр. рас-тв действительных чисел, а из нее по теореме Больцано-Вейерштрасса можно выбрать с.с.с. подрас-тв $x_{n_k} \rightarrow x_0$

Аналогично выберем $y_{n_k} \rightarrow y_0$ (y_{n_k} подпослед-ть y_{n_k} (соотв-ая x_{n_k})).

▲ Тогда соотв-ая подрас-тв $z_{n_k} \rightarrow z_0 = x_0 + iy_0$

Лемма 6. Точная нижняя грань модуля многочлена достижима, т.е. $\exists z_0 : |f(z_0)| \leq |f(z)|$ при $\forall z \in \mathbb{C}$.

Δ Д-во: Рассмотрим мн-во значений $|f(z)|$. Т.к. $|f(z)| \geq 0$, то это мн-во отсчитуемо $\Rightarrow$

$\exists m \in \mathbb{N} : |f(z)| = m \Rightarrow$

$\forall n \exists z_n : |f(z_n)| \leq m + \frac{1}{n}$

Из Леммы 4 для $M = m+1$ найдём R такое что при $|z| > R$ будет $|f(z)| > M \geq m + \frac{1}{n}$, а значит: $|z_n| \leq R$, т.е. z_n - ограничена $\Rightarrow$ по Лемме 5 из нее можно выбрать с.с.с. подрас-тв $z_{n_k} \rightarrow z_0$, тогда в силу непрерывности $|f(z)|$ (Лемма 3)

$$\lim_{k \rightarrow \infty} |f(z_{n_k})| = |f(z_0)|$$

Но с другой стороны:

$$m \leq |f(z_{n_k})| \leq m + \frac{1}{n_k}, \text{ по условию}$$

$$\lim_{k \rightarrow \infty} |f(z_{n_k})| = m;$$

А значит: $|f(z_0)| = m.$

Лемма I (Лемма Заномбергера)

Если $f(z)$ - многочлен степени $n \geq 1$ и $f(z_0) \neq 0$,
то $\exists z_1: |f(z_1)| < |f(z_0)|$.

Док-во: Разложим $f(z)$ по степеням Δ

$z - z_0$: $f(z) = c_0 + c_1(z - z_0) + \dots + c_n(z - z_0)^n; (*)$

Очевидно, что $c_0 = f(z_0) \neq 0$. Пусть c_k - первый ненулевой коэффициент в $(*)$ после c_0 . (он $\exists$, т.к. $f(z)$ - не константа).

Тогда: $f(z) = c_0 + c_k(z - z_0)^k + c_{k+1}(z - z_0)^{k+1} + \dots + c_n(z - z_0)^n = c_0 \left(1 + \frac{c_k}{c_0}(z - z_0)^k + \frac{c_{k+1}}{c_0}(z - z_0)^{k+1} + \dots + \frac{c_n}{c_0}(z - z_0)^n \right)$

$$= c_0 \left(1 + \frac{c_k}{c_0}(z - z_0)^k + \frac{c_k}{c_0}(z - z_0)^k g(z - z_0) \right), \quad (1)$$

где $g(z - z_0) = \frac{c_{k+1}}{c_k}(z - z_0) + \dots + \frac{c_n}{c_k}(z - z_0)^{n-k}$ -
многочлен от $z - z_0$ с нулевым свод. членом.

Согласно Лемме 1, для $\varepsilon = \frac{1}{2}$ $\exists \delta$: если $|z - z_0| < \delta$,
то:

$$|g(z - z_0)| < \frac{1}{2}$$

Оценим правую часть (1): $\frac{c_k}{c_0} = R(\cos \theta + i \sin \theta)$
 $z - z_0 = r(\cos \varphi + i \sin \varphi)$ выберем n так,
чтобы $R r^n < 1$, где этого всегда

$r < \sqrt[1/R]{1/R}$ где $\theta + k\gamma = \pi$, т.е.
возьмем $\gamma = (\pi - \theta)/k$

при малом δ .

$$\left[\frac{C_k}{C_0} = (z - z_0)^k = -Rr^k \right]$$

Теперь положим $z_1 = z_0 + r(\cos \gamma + i \sin \gamma)$
при $r < \min(\delta, \sqrt[1/R]{1/R})$ и $\gamma = \frac{\pi - \theta}{k}$,

Тогда:

$$F(z_1) = C_0 (1 - Rr^k - Rr^k g(z_1, -z_0))$$

Оценим $|F(z)| = |C_0| \cdot |1 - Rr^k - Rr^k g(z_1, -z_0)| \leq$
 $\leq |C_0| (|1 - Rr^k| + Rr^k |g(z_1, -z_0)|) \leq$
 $\leq \{ \delta \text{ и } \log \text{ для } r \text{ и } |g(z_1, -z_0)| \leq \frac{1}{2} \} \leq$
 $\leq |C_0| (1 - Rr^k + \frac{Rr^k}{2}) = |C_0| (1 - \frac{Rr^k}{2}) <$
 $< |C_0| = |F(z_0)|$



Док-во основной теоремы ансбры:

$f(z)$ — многоч. непрерывен на $\mathbb{C}$ и $n \geq 1$ раз ∞ на $\mathbb{C}$
 от ∞ к ∞ $\mathbb{C}$

по Лемме 6 $|f(z)|$ имеет $\inf |f(z)| = m$,
 которая достигается в m . z_0 так что $|f(z_0)| = m$;

Тогда $|f(z_0)| = 0$, т.е. z_0 — корень

Лемма 7 $\exists$ точка z_1 : $|f(z_1)| < |f(z_0)| =$
 $= \inf |f(z)|$, что невозможно, т.о.

z_0 — корень $f(z)$ и ∞ на $\mathbb{C}$ непрерывно
 имеет ансбр. замкнуто



Теорема 2 Для любого многочлена $f(z) = \sum_{k=0}^n a_k z^k$

$f \in \mathbb{C}[z]$ степени $n \geq 1$ $\exists$ числа $c_1, c_2, \dots, c_n \in \mathbb{C}$ такие, что

$$f(z) = a_n (z - c_1) \dots (z - c_n) \quad (*)$$

Это разложение единственно с точностью до пор-на сомножителей.

До-во: I. Из ансебр. замкнутости $\mathbb{C}$ $\Rightarrow \exists c_1 \in \mathbb{C} : f(c_1) = 0 \Rightarrow$ в полье $\mathbb{C}[z]$ □

многочлен $f(z)$ делится на многочлен $z - c_1$ так что $f(z) = (z - c_1) f_1(z)$, где $f_1(z) \in \mathbb{C}[z]$, $\deg f_1 = n - 1$. Если $n - 1 \geq 1$, то к многочлену $f_1(z)$ так же применима основная теор. ансебры и зтомим

$$f(z) = (z - c_1)(z - c_2) f_2(z) \quad (f_2(z) \in \mathbb{C}[z])$$

$\deg f_2 = n - 2;$

Применив эти рассуждения n раз, получим:

$$f(z) = (z - c_1) \dots (z - c_n) \cdot f_n;$$

где $\deg f_n = 0 \Rightarrow f_n \equiv \text{const}$ сравнив коэфф. при z^n , получим: $f_n \equiv a_n$;

II. Дока-м единственность этого разложения. Пусть $\exists$ другое разложение:

$$f(z) = (z - d_1) \dots (z - d_n) a_n; \quad (**)$$

Каждое число c_i из первого разложения встречается среди чисел $d_1, \dots, d_n$ второго, т.е. иначе для $c_i \neq d_j \quad j = \overline{1, n}$ из $(*)$

Получим, что $f(c_i) = 0$, а из $(**)$ $f(c_i) \neq 0$

Аналогично каждое из d_i встречается среди $c_1, \dots, c_n$.

Покажем теперь, что если $c_i = d_j$, то c_i встречается в (*) столько раз сколько d_j встречается в (**).

Пусть $c_i = d_j$; c_i вып. в (*) ~~к~~ раз.
 d_j вып. в (**) ~~м~~ раз
 и $k > m$;

Пусть $(z - c_i)^m = \varphi(z)$;

Тогда:

$$\varphi(z)(z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) = \varphi(z) \cdot$$

А знаем:

$$\prod_{d_s \neq d_j} (z - d_s);$$

$$\varphi(z) \left[(z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) - \prod_{d_s \neq d_j} (z - d_s) \right] = 0.$$

Т.е. в конуре $C \in \mathbb{C}$ нем ген-ней 0, но

$$(z - c_i)^{k-m} \prod_{c_s \neq c_i} (z - c_s) = \prod_{d_s \neq d_j} (z - d_s).$$

Положим в этом р-ве $z = c_i$ приходим к противоречию $\Rightarrow k \leq m$

(Аналогично пока-а $k \geq m$) и в

 итоге : $k = m$.

Вопрос №26.

Каноническое разложение многочлена над $\mathbb{C}$. кратность корня.

Теорема 1. (о канон. разл. над $\mathbb{C}$)

Для $\forall$ многочлена $f(z) = \sum_{k=0}^n a_k z^k \in \mathbb{C}[z]$ степени $n \geq 1$ $\exists$ ^{много} $c_1, c_2, \dots, c_m \in \mathbb{C}$, где $c_i \neq c_j$ ($i \neq j$) и $\exists$ числа $k_1, \dots, k_m$, где $k_1 + \dots + k_m = n$, такие что:

$$(2) f(z) = a_n (z - c_1)^{k_1} (z - c_2)^{k_2} \dots (z - c_m)^{k_m};$$

Это разложение ед-ко, с точностью до пер-ка сомножителей.

Д-во:



$$f(z) = a_n (z - c_1) \dots (z - c_n); (1)$$

среди чисел $c_1, \dots, c_n$ могут быть одинаковые, пусть $c_1, \dots, c_m$ различны, а каждое из $c_{m+1}, \dots, c_n$ совпадает с одним из $c_1, \dots, c_m$. Объединив одинаковые, получим:

$$f(z) = a_n (z - c_1)^{k_1} (z - c_2)^{k_2} \dots (z - c_m)^{k_m};$$

где $c_i \neq c_j$ ($i \neq j$) по построению $k_1 + \dots + k_m = n$, т.е. $k_1 + \dots + k_m$ - число всех сомножителей в (1).

Единств-ость $\Rightarrow$ ^{ед-ств} $\exists$ разложение (1). 

Опр. Разложение (2) - каноническое. (над полем $\mathbb{C}$)
Числа c_i ($i = \overline{1, m}$) явл-я корнями
многочлена $f(z)$ (т.е. $f(c_i) = 0, i = \overline{1, m}$) и

других корней этот многочлен не имеет
(т.е. $f(x) \neq 0$ для $\forall$ числа $x \neq c_i$; $i = \overline{1, m}$)

Число k_i в каноническом разложении
называется кратностью корня c_i .

Если $k_i = 1$, то корень - простой, если
 $k_i > 1$, то корень - кратный.

Следствие 1. Любой многочлен $f(z) \in \mathbb{C}[z]$
степени $n \geq 1$ имеет ровно n корней
(считая совпадающие).

↑ Замечание Не применимо к $f(z) \equiv 0$,
т.е. у него $\forall z \in \mathbb{C}$ - корень.

Вопрос №27.

Каково минимальное разложение многочлена над полем вещ-в чисел.

$$f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{R}[x] \quad (a_n \neq 0)$$

т.ч. $\mathbb{R} \subset \mathbb{C}$, то f можно рассматривать и как многочлен над полем $\mathbb{C}$. Тогда, как показано ранее, он имеет (с учетом кратности) n корней (возможно комплексных).

Теорема 1. Если c - комплексный (и не действительный) корень $f(x) \in \mathbb{R}[x]$, то и $\bar{c}$ явл-ся корнем этого многочлена.

Док-во:

Если c корень, то $a_0 + a_1 c + \dots + a_n c^n = 0$

Взяв сопряжение от обеих частей

$[\bar{a}_k = a_k \quad (k=0, n)]$ получим:

$$a_0 + a_1 \bar{c} + \dots + a_n \bar{c}^n = 0;$$

• Получим $\varphi(x) = (x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + |c|^2$

$$\varphi(x) \in \mathbb{R}[x]$$

Теорема 2 Если c - комплексный (и не действительный) корень мн-ка $f(x) \in \mathbb{R}[x]$, то в кольце $\mathbb{R}[x]$ мн-н $f(x)$ дел-ся на $\varphi(x)$.

Д-во: $f(x) = \varphi(x)q(x) + r(x);$

$[q(x), r(x) \in \mathbb{R}[x]]$, но это же деление

можно рассматривать и в $\mathbb{C}[x]$, тогда

$f(x)$ делится на $\varphi(x)$, т.ч. c и $\bar{c}$ - его корни ($f(x)$), а т.ч. результатом деления

$f(x)$ на $y(x)$ единствен, получим:
 $f(x) = q(x) \cdot y(x)$. ($q(x) \in \mathbb{R}[x]$)

Теорема 3 кратности корней c и $\bar{c}$ многочлена с вещ-ми коэфф. совпадают.

□ До-во: Пусть c и $\bar{c}$ - корни $f(x) \in \mathbb{R}[x]$; кратности m и k (сооб-но)

Пусть $k > m$, тогда:

$f(x) = (y(x))^m \cdot q(x)$, где $q(x) \in \mathbb{R}[x]$; но $q(c) = 0$, а $q(\bar{c}) \neq 0$, что невозможно в силу Теоремы 1, значит $k \leq m$.

Аналогично можно показ-ть: $m \leq k$,

А значит: $m = k$.

Следствие: Многочлен с вещ-ми коэфф. нечетной степени имеет хотя бы один корень (вещ-ый)

Теорема 4 (о каноническом разлож. многочлена над полем $\mathbb{R}$)

Для $\forall$ многочлена $f(x) = \sum_{k=0}^n a_k x^k \in \mathbb{R}[x]$ степени $n \geq 1$, $\exists$ числа $c_1, \dots, c_r \in \mathbb{R}$, где $c_i \neq c_j$ ($i \neq j$); числа $p_1, q_1, \dots, p_s, q_s \in \mathbb{R}$, где $(p_i, q_i) \neq (p_j, q_j)$ ($i \neq j$); числа $k_1, \dots, k_r \in \mathbb{N}$ и $l_1, \dots, l_s \in \mathbb{N}$, где $\sum_{i=1}^r k_i + 2 \cdot \sum_{j=1}^s l_j = n$, такие что:

$$(*) \quad f(x) = a_n \prod_{i=1}^r (x - c_i)^{k_i} \cdot \prod_{j=1}^s (x^2 + p_j x + q_j)^{l_j};$$

Доказательство: Умножение разложения



$$(1) f(x) = a_n (x - c_1)^{k_1} \dots (x - c_m)^{k_m} \quad \left(\begin{array}{l} \text{раскл. } f(x), \\ \text{на множители,} \\ \text{комп.} \\ \text{и сф.} \end{array} \right)$$

$\forall i: c_i \neq c_j \ (i \neq j);$
 $k_1 + \dots + k_m = n;$

Числа $c_1, \dots, c_m$ явл-ся корнями (комплексными) $f(x)$. Среди этих корней могут быть и действительные. Пусть $c_1, \dots, c_r$ - действительные, а $c_{r+1}, \dots, c_m$ - комплексные (не действительные). Тогда среди $c_{r+1}, \dots, c_m$ вместе с каждым корнем c_j найдётся и сопряжённый ему корень $c_i = \bar{c}_j$, причём той же кратности, так что $k_i = k_j = l_j$ а значит $2l_j = k_i + k_j$

• Объединим в (1) пары сопряжённых:

$$(x - c_j)^{k_j} \cdot (x - c_i)^{k_i} = ((x - c_j)(x - \bar{c}_j))^{l_j} = (x^2 + p_j x + q_j)^{l_j}, \text{ где}$$
$$p_j = -(c_j + \bar{c}_j) \in \mathbb{R}; \quad q_j = c_j \bar{c}_j \in \mathbb{R}$$

• Тогда: $(x - c_{r+1}) \dots (x - c_m) = (x^2 + p_1 x + q_1)^{l_1} \dots (x^2 + p_s x + q_s)^{l_s}$ а разложение (1) перейдет в (*), причём:

$$k_1 + \dots + k_r + 2(l_1 + \dots + l_s) = k_1 + \dots + k_m = n;$$

Замечание: Теорема о р-ве многочленов справедлива и для вещ-ых (если рассм-ть их, как комплексное). Формулы Виета справедливы лишь для тех мн-ов из $\mathbb{R}[x]$, которые имеют полный набор действ. корней.

Вопрос № 28.

Формулы Виета. Линейные мн-ва.

Теорема 1 (Ф-мы Виета)

Если $c_1, \dots, c_n$ - корни $f(z) = \sum_{k=0}^n a_k z^k$, то

$$(1) \begin{cases} \frac{a_{n-1}}{a_n} = -(c_1 + c_2 + \dots + c_n); \\ \frac{a_{n-2}}{a_n} = +(c_1 c_2 + c_1 c_3 + \dots + c_1 c_n + c_2 c_3 + \dots + c_{n-1} c_n); \\ \dots \\ \frac{a_{n-k}}{a_n} = (-1)^k \sum_{i_1 < i_2 < \dots < i_k} c_{i_1} c_{i_2} \dots c_{i_k}; \\ \dots \\ \frac{a_0}{a_n} = (-1)^n c_1 \dots c_n; \end{cases}$$

Доказ-во: Демонстрируем рассуждениями. $\square$

$a_n = 1$ [$F(z)$ и $\frac{1}{a_n} F(z)$ имеют один. корни]

Умозаключаем по n :

1) Для $n=2$ Ф-мы Виета яв-ся след-ствием из 3-х-ой алгебры.

2) Пусть для мн-ва $(n-1)$ степени Ф-мы (1) имеют место, докажем их для мн-ва $f(z) = a_0 + a_1 z + \dots + a_{n-1} z^{n-1} + z^n$.

Разн-ие: $f(z) = ((z - c_1) \dots (z - c_{n-1})) \cdot (z - c_n) =$
(линейное) $= g(z) \cdot (z - c_n)$

Где $g(z) = (z - c_1) \dots (z - c_{n-1})$ - мн-н степени $n-1$

Пусть $g(z) = b_0 + b_1 z + \dots + b_{n-2} z^{n-2} + z^{n-1}$

Тогда:

$$f(z) = (b_0 + b_1 z + \dots + b_{n-2} z^{n-2} + z^{n-2}).$$

$$\cdot (z - c_n) =$$

$$= b_0 z + b_1 z^2 + \dots + b_{n-2} z^{n-1} + z^n - (b_0 c_n + b_1 c_n z + \dots + b_{n-2} c_n z^{n-2} + c_n z^{n-1})$$

$$\equiv -b_0 c_n + (b_0 - b_1 c_n) z + \dots + (b_{n-k-1} - b_{n-k} c_n) \cdot z^{n-k} + \dots + z^n.$$

$$f(z) = a_0 + a_1 z + \dots + a_{n-k} z^{n-k} + \dots + z^n$$

Сравним коэффициенты при z^{n-k} и увидим, что для b_i ($i = 0, n-2$) верно соотношение (1), т.е.

$$b_{(n-1)-k} = (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq n-1} c_{i_1} c_{i_2} \dots c_{i_k}$$

Тогда:

$$a_{n-k} = b_{n-k-1} - b_{n-k} c_n =$$

$$= b_{(n-1)-k} - b_{(n-1)-(k-1)} c_n =$$

$$= (-1)^k \cdot \sum_{1 \leq i_1 < \dots < i_k \leq n-1} c_{i_1} \dots c_{i_k} - (-1)^k c_n \sum_{1 \leq i_1 < \dots < i_{k-1} \leq n-1} c_{i_1} \dots c_{i_{k-1}} =$$

$$= (-1)^k \cdot \left(\sum_{1 \leq i_1 < \dots < i_k \leq n} c_{i_1} \dots c_{i_k} - \sum_{1 \leq i_1 < \dots < i_{k-1} \leq n} c_{i_1} \dots c_{i_{k-1}} \right) =$$

$$= (-1)^k \cdot \left(\sum_{1 \leq i_1 < \dots < i_k \leq n} c_{i_1} \dots c_{i_k} \right)$$

Замечание: Все упр-ия имеют место в V алгебр замкнутом поле.

Опр. Такие многочлены от пер-ых $x_1, \dots, x_n$, которые не меняются ни при какой перестановке корней $x_1, \dots, x_n$ наз-ся Симметрическими многочленами.

Элементарные симметр. мн-ты:

$$\sigma_1 = x_1 + \dots + x_n;$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n;$$

$$\sigma_{n-k}^{\dots} = \sum_{i_1 < \dots < i_k} x_{i_1} x_{i_2} \dots x_{i_k};$$

$$\sigma_n^{\dots} = x_1 \dots x_n;$$

Дополнительно:

Опр Характеристический многочлен матрицы $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ наз-ся φ -ция $f(\lambda) = |A - \lambda I|$;

а) $n=2 \Leftrightarrow f(\lambda) = (-\lambda)^2 + a_1(-\lambda) + a_0$

$a_1 = \text{tr} A$; $a_0 = |A|$;

б) $n=3 \Leftrightarrow f(\lambda) = (-\lambda)^3 + a_2(-\lambda^2) + a_1(-\lambda) + a_0$

$a_2 = \text{tr} A$; $a_1 = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$;

Опр Главные миноры матрицы наз-ся минор, расположенный в строках и столбцах с одинаковыми номерами.

в а): a_1 - сумма Гл. мин. 1-го пор, a_0 - ед.

в б) a_2 --- 1-го пор

Гл. минор 2-го пор

a_1 --- 2-го

a_0 --- 3-го

Опр Матрицы $A, B \in \mathbb{R}^{n \times n}$ наз-ся подобными, если суц-ет невырожденная матр. Q такая, что: $A = Q^{-1} B Q$

Теорема 1. Хар-е многочлены подобных матриц совпадают.

Док-во: Если $A = Q^{-1} B Q$, то



$$|A - \lambda I| = |Q^{-1} B Q - \lambda I| \Leftrightarrow$$

$$\begin{aligned} &\equiv |Q^{-1}BQ - Q^{-1}\lambda I Q| = \\ &= |Q^{-1}(B - \lambda I)Q| = |B - \lambda I|; \end{aligned}$$

Следствие: У подобных матриц 2го
 порядка совпадают следы и опред-ли.
 У подобных матриц 3го пор-ка совпадают
 следы, суммы главных миноров 2го
 пор-ка и опред-ли.

Построение конечных полей.

Для $GF(2^2)$:

1) Над полем $\mathbb{Z}_2$ находим непривод. многочлен степени 2: $x^2 + x + 1$

2) Поле $GF(2^2)$ - факторкольцо $\mathbb{Z}_2[x] / (x^2 + x + 1) = \mathbb{K}$;

Эл-ты $\mathbb{K}$ можно представить как многочлены с коэф. из $\mathbb{Z}_2$ степени не выше 2, т.е.:

$$0, 1, x+1, x$$

Сложение: по модулю 2

Умножение: по модулю 2, в качестве д-ля

Берем остаток от дел-ия на $x^2 + x + 1$

(Получим везде $x^2 = -x-1$, но т.к. в $\mathbb{Z}_2$ $-1=1$, то $x^2 = x+1$).